(Translation of the front page
of the priority document of
Japanese Patent Application
No. 2001-161403)

PATENT OFFICE
JAPANESE GOVERNMENT

This is to certify that the annexed is a true copy of the following application as filed with this Office.

Date of Application : April 23, 2001

Application Number : Patent Application
2001-161403

Applicant(s) : Humming Heads Inc.

November 9, 2001

Commissioner,
Japan Patent Office Kouzo Oikawa

Certification Number 2001-3098288

日　本　国　特　許　庁
JAPAN PATENT OFFICE

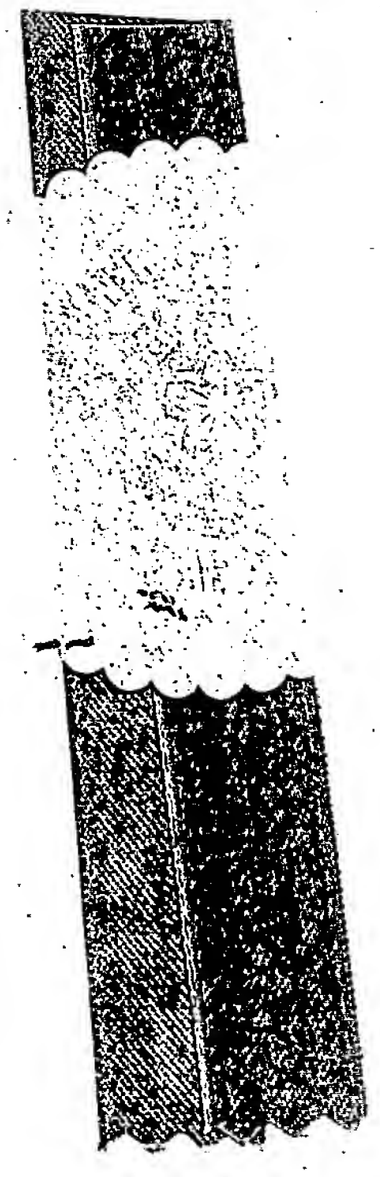
別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２００１年　４月２３日

出願番号
Application Number: 特願２００１－１６１４０３

出願人
Applicant(s): ハミングヘッズ株式会社



２００１年１１月　９日

特許庁長官
Commissioner,
Japan Patent Office

及川耕造

出証番号　出証特２００１－３０９８２８８

【書類名】　特許願

【整理番号】　HH08PH1301

【提出日】　平成13年 4月23日

【あて先】　特許庁長官殿

【国際特許分類】　G06F 17/00

【発明者】

【住所又は居所】　東京都中央区月島一丁目２番１３号　ハミングヘッズ株式会社内

【氏名】　大江　尚之

【発明者】

【住所又は居所】　東京都中央区月島一丁目２番１３号　ハミングヘッズ株式会社内

【氏名】　志摩　貴浩

【特許出願人】

【識別番号】　500083226

【住所又は居所】　東京都中央区月島一丁目２番１３号

【氏名又は名称】　ハミングヘッズ株式会社

【代表者】　大江　尚之

【電話番号】　03-3531-7281

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【先の出願に基づく優先権主張】

【出願番号】　特願2000-352113

【出願日】　平成12年11月20日

【書類名】　　明細書

【発明の名称】　コンピュータリソースの制御方法および装置並びに記録媒体

【特許請求の範囲】

【請求項１】　ファイル、ネットワーク、記憶装置、表示画面、外部付属装置等のオペレーティングシステムが管理しているコンピュータリソースに対するアクセスを制御する方法であって、

前記コンピュータリソースに対するプロセスまたはオペレーティングシステムからの操作要求をコンピュータリソースにアクセスする前に捕捉する第１のステップと、

前記第１のステップで捕捉した操作要求によって指定されるコンピュータリソースに対するアクセス権限があるか否かを判定する第２のステップと、

アクセス権限があれば当該操作要求通りにオペレーティングシステムに渡し、その結果を要求元プロセスに返す第３のステップと、

アクセス権限がなければ当該操作要求を拒否する第４のステップと

を備えることを特徴とするコンピュータリソースの制御方法。

【請求項２】　前記第１のステップに代えて、前記コンピュータリソースに対するプロセス及びオペレーティングシステムからの操作要求をコンピュータリソースにアクセスする前に捕捉する第５のステップを備えることを特徴とする請求項１に記載のコンピュータリソースの制御方法。

【請求項３】　前記第２のステップが、

特定のコンピュータリソースを指定するリソース指定情報、アクセス権が有効となる条件情報、既存環境で定義されていない拡張したアクセス権を指定するアクセス権限情報を含むアクセス権管理テーブルを参照し、アクセス権限があるか否かを判定するステップまたは、

コンピュータリソース内部に記述された、既存環境で定義されていない拡張したアクセス権を指定するアクセス権限情報を参照し、アクセス権限があるか否かを判定するステップまたは、

アクセス権限が獲得できたか否かをもって、アクセス権限があるか否かを判定するステップ

を備えることを特徴とする請求項１または２に記載のコンピュータリソースの制御方法。

【請求項４】　前記アクセス権限情報は、他媒体への移動権限、他媒体へのコピー権限、印刷権限、共有メモリへの読み込み権限、画面ハードコピー権限、使用プロセスの限定権限のうち少なくとも１つを指定する情報を含むことを特徴とする請求項３に記載のコンピュータリソースの制御方法。

【請求項５】　前記第４のステップは、

要求されたコンピュータリソースにアクセスせずにアクセス違反のエラー通知を要求元プロセスに返す、または要求されたコンピュータリソースにアクセスせずにアクセス成功の通知を要求元プロセスに返す、またはダミーのコンピュータリソースへの操作要求に変換してオペレーティングシステムに渡し、その結果を要求元プロセスに返すステップから成ることを特徴とする請求項１～４のいずれか一項に記載のコンピュータリソースの制御方法。

【請求項６】　ファイル、ネットワーク、記憶装置、表示画面、外部付属装置等のオペレーティングシステムが管理しているコンピュータリソースに対するアクセスを制御するリソース制御手段を備えたコンピュータ装置であって、

前記リソース制御手段が、

前記コンピュータリソースに対するプロセスまたはオペレーティングシステムからの操作要求をコンピュータリソースにアクセスする前に捕捉する第１の手段と、

前記第１の手段で捕捉した操作要求によって指定されるコンピュータリソースに対するアクセス権限があるか否かを判定する第２の手段と、

アクセス権限があれば当該操作要求通りにオペレーティングシステムに渡し、その結果を要求元プロセスに返す第３の手段と、

アクセス権限がなければ当該操作要求を拒否する第４の手段と

を備えることを特徴とするコンピュータ装置。

【請求項７】　前記第１の手段に代えて、前記コンピュータリソースに対するプロセス及びオペレーティングシステムからの操作要求をコンピュータリソースにアクセスする前に捕捉する第５の手段を備えることを特徴とする請求項６に

記載のコンピュータ装置。

【請求項８】　前記第２の手段が、

特定のコンピュータリソースを指定するリソース指定情報、アクセス権が有効となる条件情報、既存環境で定義されていない拡張したアクセス権を指定するアクセス権限情報を含むアクセス権管理テーブルを参照し、アクセス権限があるか否かを判定する手段または、

コンピュータリソース内部に記述された、既存環境で定義されていない拡張したアクセス権を指定するアクセス権限情報を参照し、アクセス権限があるか否かを判定する手段または、

アクセス権限が獲得できたか否かをもって、アクセス権限があるか否かを判定する手段

を備えることを特徴とする請求項６または７に記載のコンピュータ装置。

【請求項９】　前記アクセス権限情報は、他媒体への移動権限、他媒体へのコピー権限、印刷権限、共有メモリへの読み込み権限、画面ハードコピー権限、使用プロセスの限定権限のうち少なくとも１つを指定する情報を含むことを特徴とする請求項８に記載のコンピュータ装置。

【請求項１０】　前記第４の手段は、

要求されたコンピュータリソースにアクセスせずにアクセス違反のエラー通知を要求元プロセスに返す、または要求されたコンピュータリソースにアクセスせずにアクセス成功の通知を要求元プロセスに返す、またはダミーのコンピュータリソースへの操作要求に変換してオペレーティングシステムに渡し、その結果を要求元プロセスに返す手段から成ることを特徴とする請求項６～９のいずれか一項に記載のコンピュータ装置。

【請求項１１】　ファイル、ネットワーク、記憶装置、表示画面、外部付属装置等のコンピュータリソースに対するアクセスを制御するリソース制御プログラムを記録した媒体であって、

前記リソース制御プログラムが、

前記コンピュータリソースに対するプロセスまたはオペレーティングシステムからの操作要求をコンピュータリソースにアクセスする前に捕捉する第１の処理

と、

前記第１の処理で捕捉した操作要求によって指定されるコンピュータリソースに対するアクセス権限があるか否かを判定する第２の処理と、

アクセス権限があれば当該操作要求通りにオペレーティングシステムに渡し、その結果を要求元プロセスに返す第３の処理と、

アクセス権限がなければ当該操作要求を拒否する第４の処理と

を備えることを特徴とするコンピュータが読取り可能なプログラムを記録した記録媒体。

【請求項１２】　前記第１の処理に代えて、前記コンピュータリソースに対するプロセス及びオペレーティングシステムからの操作要求をコンピュータリソースにアクセスする前に捕捉する第５の処理を備えることを特徴とする請求項１１に記載の記録媒体。

【請求項１３】　前記第２の処理が、

特定のコンピュータリソースを指定するリソース指定情報、アクセス権が有効となる条件情報、既存環境で定義されていない拡張したアクセス権を指定するアクセス権限情報を含むアクセス権管理テーブルを参照し、アクセス権限があるか否かを判定する処理または、

コンピュータリソース内部に記述された、既存環境で定義されていない拡張したアクセス権を指定するアクセス権限情報を参照し、アクセス権限があるか否かを判定する処理または、

アクセス権限が獲得できたか否かをもって、アクセス権限があるか否かを判定する処理

を備えることを特徴とする請求項１１または１２に記載の記録媒体。

【請求項１４】　前記アクセス権限情報は、他媒体への移動権限、他媒体へのコピー権限、印刷権限、共有メモリへの読み込み権限、画面ハードコピー権限、使用プロセスの限定権限のうち少なくとも１つを指定する情報を含むことを特徴とする請求項１３に記載の記録媒体。

【請求項１５】　前記第４の処理は、

要求されたコンピュータリソースにアクセスせずにアクセス違反のエラー通知

を要求元プロセスに返す、または要求されたコンピュータリソースにアクセスせずにアクセス成功の通知を要求元プロセスに返す、またはダミーのコンピュータリソースへの操作要求に変換してオペレーティングシステムに渡し、その結果を要求元プロセスに返す処理から成ることを特徴とする請求項１１～１４のいずれか一項に記載の記録媒体。

【請求項１６】　ファイル、ネットワーク、記憶装置、表示画面、外部付属装置等のコンピュータリソースに対するアクセスを制御するリソース制御プログラムであって、

前記コンピュータリソースに対するプロセスまたはオペレーティングシステムからの操作要求をコンピュータリソースにアクセスする前に捕捉する第１の処理と、

前記第１の処理で捕捉した操作要求によって指定されるコンピュータリソースに対するアクセス権限があるか否かを判定する第２の処理と、

アクセス権限があれば当該操作要求通りにオペレーティングシステムに渡し、その結果を要求元プロセスに返す第３の処理と、

アクセス権限がなければ当該操作要求を拒否する第４の処理と

を備えることを特徴とするコンピュータが実行可能なリソース制御プログラム。

【請求項１７】　前記第１の処理に代えて、前記コンピュータリソースに対するプロセス及びオペレーティングシステムからの操作要求をコンピュータリソースにアクセスする前に捕捉する第５の処理を備えることを特徴とする請求項１６に記載のリソース制御プログラム。

【請求項１８】　前記記載の処理においてアクセス権限がないと判定され、アクセスを拒否された場合課金することによってアクセス権限を許可することを特徴とするリソース制御プログラム。

【請求項１９】　前記記載のコンピュータリソースとは、ウエブキャスト、デジタル放送、音楽配信等のコンテンツを含むことを特徴とするリソース制御プログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、ファイル、記憶装置、表示画面、外部付属装置等のコンピュータリソースに対するアクセスを管理するコンピュータリソースの制御方法および装置並びに記録媒体に関するものである。

【０００２】

【従来の技術】

従来において、パーソナルコンピュータ等のコンピュータにおけるファイルや記憶装置等のリソースをアプリケーションプログラムを介してユーザがアクセスする場合に、アクセス権限のないユーザに情報が解読または盗聴されるのを防ぐために、オペレーティングシステム（以下、ＯＳ）内にアクセス権限のチェック機能を設ける方法、あるいは専用のアクセス管理ツールを付加してアクセス権限のチェックを行なう方法が知られている。

【０００３】

例えばＷｉｎｄｏｗｓ（米国マイクロソフト社の登録商標）に代表される汎用のＯＳにおいては、ファイルの読取り、書き込み、実行をアクセス権限のないユーザに対しては許可しない機能が備わっている。また、ファイルの削除、アクセス権限の変更、所有権の変更についての権限を設定可能にした汎用ＯＳもある。

また、アクセス管理ツールとして、例えば特開平７－８４８５２公報に開示されているように、ファイルの参照と共に複写の可否を登録し、その可否によって参照、複写を制限するものが知られている。詳しくは、表示領域に読出し制限の属性を付加し、表示画面のハードコピーを防止するものが知られている。

【０００４】

【発明が解決しようとする課題】

アクセス権限のないユーザに対して情報の持ち出しを全面的に禁止するためには、図９に示すように、メールへの添付、印刷、ファイル移動／ファイルコピー、クリップボードへのコピー、フロッピーディスクへの別名保存、オブジェクトの貼り付け、画面ハードコピーなどの機能を制限する必要がある。さらに、ネットワークを通じた情報の持ち出しを制限する必要がある。

しかしながら、上記従来技術にあっては、ファイル及び画面のハードコピー以

外の操作（例えばクリップボードへのコピー）に対して制限することができないという問題がある。もしも、クリップボードへのコピーなどの操作を制限しようとする場合には、ＯＳまたはアプリケーション自体に変更を加えることが必要になり、汎用的な応用ができないという問題がある。

【０００５】

本発明の目的は、ＯＳやプロセス（ＯＳの元に稼動しているプログラムであり、アプリケーションやデーモンなど）を変更することなく、ファイルや画面以外のコンピュータリソースを含めてアクセス権限のないユーザに対するリソースの操作を制限し、しかも既存環境における禁止または制限事項を拡張することができるコンピュータリソースの制御方法および装置並びに記録媒体を提供することにある。

【０００６】

【課題を解決するための手段】

上記目的を達成するために、本発明のコンピュータリソースの制御方法は、ファイル、ネットワーク、記憶装置、表示画面、外部付属装置等のオペレーティングシステムが管理しているコンピュータリソースに対するプロセスまたはオペレーティングシステムからの操作要求をコンピュータリソースにアクセスする前に捕捉する第１のステップと、前記第１のステップで捕捉した操作要求によって指定されるコンピュータリソースに対するアクセス権限があるか否かを判定する第２のステップと、アクセス権限があれば当該操作要求通りにオペレーティングシステムに渡し、その結果を要求元プロセスに返す第３のステップと、アクセス権限がなければ当該操作要求を拒否する第４のステップとを備えることを特徴とする。

また、前記第１のステップに代えて、前記コンピュータリソースに対するプロセス及びオペレーティングシステムからの操作要求をコンピュータリソースにアクセスする前に捕捉する第５のステップを備えることを特徴とする。

また、前記第２のステップが、特定のコンピュータリソースを指定するリソース指定情報、アクセス権が有効となる条件情報、既存環境で定義されていない拡張したアクセス権を指定するアクセス権限情報を含むアクセス権管理テーブルを

参照し、アクセス権限があるか否かを判定するステップ、またはコンピュータリソース内部に記述された既存環境で定義されていない拡張したアクセス権を指定するアクセス権限情報を参照し、アクセス権限があるか否かを判定するステップ、またはアクセス権限が獲得できたか否かをもって、アクセス権限があるか否かを判定するステップを備えることを特徴とする。

また、前記アクセス権限情報は、他媒体への移動権限、他媒体へのコピー権限、印刷権限、共有メモリへの読み込み権限、画面ハードコピー権限、使用プロセスの限定権限のうち少なくとも１つを指定する情報を含むことを特徴とする。

また、前記第４のステップは、要求されたコンピュータリソースにアクセスせずにアクセス違反のエラー通知を要求元プロセスに返す、または要求されたコンピュータリソースにアクセスせずにアクセス成功の通知を要求元プロセスに返す、またはダミーのコンピュータリソースへの操作要求に変換してオペレーティングシステムに渡し、その結果を要求元プロセスに返すステップから成ることを特徴とする。

【０００７】

さらに、コンピュータリソースに対するアクセスを制御するリソース制御手段を備えた本発明に係るコンピュータ装置は、

前記リソース制御手段が、

前記コンピュータリソースに対するプロセスまたはオペレーティングシステムからの操作要求をコンピュータリソースにアクセスする前に捕捉する第１の手段と、前記第１の手段で捕捉した操作要求によって指定されるコンピュータリソースに対するアクセス権限があるか否かを判定する第２の手段と、アクセス権限があれば当該操作要求通りにオペレーティングシステムに渡し、その結果を要求元プロセスに返す第３の手段と、アクセス権限がなければ当該操作要求を拒否する第４の手段とを備えることを特徴とする。

また、前記第１の手段に代えて、前記コンピュータリソースに対するプロセス及びオペレーティングシステムからの操作要求をコンピュータリソースにアクセスする前に捕捉する第５の手段を備えることを特徴とする。

また、前記第２の手段が、特定のコンピュータリソースを指定するリソース指

定情報、アクセス権が有効となる条件情報、既存環境で定義されていない拡張したアクセス権を指定するアクセス権限情報を含むアクセス権管理テーブルを参照し、アクセス権限があるか否かを判定する手段、またはコンピュータリソース内部に記述された、既存環境で定義されていない拡張したアクセス権を指定するアクセス権限情報を参照し、アクセス権限があるか否かを判定する手段、またはアクセス権限が獲得できたか否かをもって、アクセス権限があるか否かを判定する手段を備えることを特徴とする。

また、前記アクセス権限情報は、他媒体への移動権限、他媒体へのコピー権限、印刷権限、共有メモリへの読み込み権限、画面ハードコピー権限、使用プロセスの限定権限のうち少なくとも１つを指定する情報を含むことを特徴とする。

また、前記第４の手段は、要求されたコンピュータリソースにアクセスせずにアクセス違反のエラー通知を要求元プロセスに返す、または要求されたコンピュータリソースにアクセスせずにアクセス成功の通知を要求元プロセスに返す、またはダミーのコンピュータリソースへの操作要求に変換してオペレーティングシステムに渡し、その結果を要求元プロセスに返す手段から成ることを特徴とする。

【０００８】

さらに本発明に係るリソース制御プログラムを記録した媒体は、前記リソース制御プログラムが、

前記コンピュータリソースに対するプロセスまたはオペレーティングシステムからの操作要求をコンピュータリソースにアクセスする前に捕捉する第１の処理と、前記第１の処理で捕捉した操作要求によって指定されるコンピュータリソースに対するアクセス権限があるか否かを判定する第２の処理と、アクセス権限があれば当該操作要求通りにオペレーティングシステムに渡し、その結果を要求元プロセスに返す第３の処理と、アクセス権限がなければ当該操作要求を拒否する第４の処理とを備えることを特徴とする。

また、前記第１の処理に代えて、前記コンピュータリソースに対するプロセス及びオペレーティングシステムからの操作要求をコンピュータリソースにアクセスする前に捕捉する第５の処理を備えること特徴とする。

また、前記第２の処理が、特定のコンピュータリソースを指定するリソース指定情報、アクセス権が有効となる条件情報、既存環境で定義されていない拡張したアクセス権を指定するアクセス権限情報を含むアクセス権管理テーブルを参照し、アクセス権限があるか否かを判定する処理、またはコンピュータリソース内部に記述された、既存環境で定義されていない拡張したアクセス権を指定するアクセス権限情報を参照し、アクセス権限があるか否かを判定する処理、またはアクセス権限が獲得できたか否かをもって、アクセス権限があるか否かを判定する処理を備えることを特徴とする。

また、前記アクセス権限情報は、他媒体への移動権限、他媒体へのコピー権限、印刷権限、共有メモリへの読み込み権限、画面ハードコピー権限、使用プロセスの限定権限のうち少なくとも１つを指定する情報を含むことを特徴とする。

また、前記第４の処理は、要求されたコンピュータリソースにアクセスせずにアクセス違反のエラー通知を要求元プロセスに返す、または要求されたコンピュータリソースにアクセスせずにアクセス成功の通知を要求元プロセスに返す、またはダミーのコンピュータリソースへの操作要求に変換してオペレーティングシステムに渡し、その結果を要求元プロセスに返す処理から成ることを特徴とする。

【０００９】

さらにコンピュータリソースに対するアクセスを制御する本発明に係るリソース制御プログラムは、前記コンピュータリソースに対するプロセスまたはオペレーティングシステムからの操作要求をコンピュータリソースにアクセスする前に捕捉する第１の処理と、前記第１の処理で捕捉した操作要求によって指定されるコンピュータリソースに対するアクセス権限があるか否かを判定する第２の処理と、アクセス権限があれば当該操作要求通りにオペレーティングシステムに渡し、その結果を要求元プロセスに返す第３の処理と、アクセス権限がなければ当該操作要求を拒否する第４の処理とを備えることを特徴とする。

発明者は本装置をＨ．Ｈコンピュータセキュリテイ方式と命名した。

【００１０】

【発明の実施の形態】

【第１実施形態】

以下、本発明の実施の形態を図面により詳細に説明する。

図１（ａ），（ｂ）は本発明を実施する環境の一実施の形態を示すハードウェア構成図である。

図１（ａ）に示す構成は、スタンドアロン構成におけるコンピュータ１０１のハード構成を示すものであり、ハードディスク（ＨＤＤ）１０１１を備えたパーソナルコンピュータ（ＰＣ）１０１２、ディスプレイ１０１３、プリンタ１０１４、外部にリソースデータを出力することが可能な外部装置１０１５で構成されている。

パーソナルコンピュータ１０１２には、汎用のＯＳとアプリケーションが組み込まれており、さらに本発明に係るリソース管理プログラムが組み込まれている。

図１（ｂ）は、ネットワーク１０２を利用する場合の構成を示すものであり、図１（ａ）に示したのと同様な構成のコンピュータ１０１ａ～１０１ｃがネットワーク１０２で接続されている。

【００１１】

このような構成において、一般的に、アプリケーションがＯＳの管理するリソースにアクセスするには、ＯＳが提供するＡＰＩ（Ａｐｐｌｉｃａｔｉｏｎ　Ｐｒｏｇｒａｍ　Ｉｎｔｅｒｆａｃｅ）を利用する。このＡＰＩの利用方法はＯＳにより確定しており、ＡＰＩを利用する実行コード部を判別することができる。本発明では、リソースへのアクセスに必要なすべてのＡＰＩを監視する監視ルーチンを設け、アプリケーションがＡＰＩを利用する前に、その実行コード部を変更するか、ＡＰＩ処理の入り口を監視ルーチンと置き換えることで、ＡＰＩ利用時に監視ルーチンが利用されるようにする。監視ルーチンは、アプリケーションが求めるＡＰＩを処理するか、もしくはＡＰＩの処理をせずに不正命令としてアプリケーションに結果を返す。本発明のリソース管理プログラムによって拡張したアクセス権の管理は、ＯＳの管理とは別に本プログラムが管理し、アクセス権の種類別に監視ルーチンを設ける。この方法により、リソースを不正に利用するアプリケーションから、そのアクセスを制限する。

【００１２】

図２は、本発明に係るリソース管理プログラム２０３の構成及びＡＰＩ監視／制御の概念を示す図であり、リソース管理プログラム２０３はＡＰＩ監視コントローラ（ＡＰＩ監視ＣＴＲＬ）２０３１、ＡＰＬ監視コントローラ（ＡＰＬ監視ＣＴＲＬ）２０３２、アクセス制御コントローラ（アクセス制御ＣＴＲＬ）２０３３、ＯＳ監視コントローラ（ＯＳ監視ＣＴＲＬ）２０３４から構成されており、リソースアクセス要求を出すアプリケーション２０２１や画面キャプチャなどのＯＳ機能操作２０２２を備える一般的なアプリケーションからなるユーザ環境２０２と汎用ＯＳ２０１との間に位置し、汎用ＯＳ２０１およびユーザ環境２０２が提供するリソースに対する要求を監視するようになっている。

なお、汎用ＯＳ２０１は、ＯＳが管理するリソース２０１１と、ＯＳがアプリケーション２０２１に提供しているＡＰＩ群２０１２を備える。

【００１３】

本発明に係るリソース管理プログラム２０３におけるＡＰＩ監視ＣＴＲＬ２０３１は、アクセス制御を行なうのに必要な全てのＡＰＩを監視するモジュールである。また、ＡＰＬ監視ＣＴＲＬ２０３２は、アプリケーション２０２１が保持しているリソースを記憶するモジュールである。アクセス制御ＣＴＲＬ２０３３はアクセスが許可されているかを判断するモジュールであり、アクセス権管理テーブル２０３５を備える。また、ＯＳ監視ＣＴＲＬ２０３４は、汎用ＯＳ２０１の機能によってリソースへアクセスする操作を監視するモジュールである。

【００１４】

アクセス権限テーブル２０３５は、図３に示すように、リソース指定情報２０３５１、条件２０３５２、ｎ個のアクセス権情報２０３５３～２０３５ｎをリソース毎に登録可能に構成されている。

リソース指定情報２０３５１は、汎用ＯＳ２０１が管理しているリソースのうち、特定のものを指定するための情報であり、例えば、ファイルの場合はファイル名やファイルＩＤなどの情報が登録される。通信データの場合は、ホスト名，ポート番号，ＩＰアドレスなどが登録され、メモリの場合は、そのオブジェクトを示すオブジェクト名，アドレスなどが登録される。また、外部出力装置の場合

は、そのデバイスドライバを示すデバイス名などが登録される。

条件２０３５２は、アクセス権が有効となる条件またはその組み合わせをしめすものであり、例えばユーザ名／ＩＤ，グループ名／ＩＤ，時刻，使用アプリケーションなどが登録される。

アクセス権情報２０３５３～２０３５ｎは、既存環境で定義されていない拡張したアクセス権のうち、指定したリソースに付加した権限を示すものであり、例えば他媒体への移動権限，他媒体へのコピー権限，印刷権限、共有メモリへの読み込み権限（Ｗｉｎｄｏｗｓではクリップボードなど），画面ハードコピー権限，使用アプリケーションの限定（特定アプリケーション以外での使用禁止やメール添付の禁止）などが登録される。

なお、一般的に、リソースへのアクセスは複数のＡＰＩによって行われることがあり、その場合はリソース指定情報はＯＳが管理するＩＤ（ハンドルなど）に変換されることがある。その場合、リソース管理プログラム２０３の内部においては、リソース指定情報とそのＩＤは同一視するようにしている。

【００１５】

このような構成に係るリソース管理プログラム２０３の処理について、図２の①～⑨で示す情報伝達手順に従って説明する。

①アプリケーション２０２１からリソースへのアクセス要求があれば、ＡＰＩ監視ＣＴＲＬ２０３１がその要求を捕捉し、アクセス制御ＣＴＲＬ２０３３に伝える。

②アクセス制御ＣＴＲＬ２０３３は、アクセス権限チェックを行なう際、必要に応じて、アプリケーション２０２１が保持しているリソースの情報をＡＰＬ監視ＣＴＲＬ２０３２から取得する。

③アクセスを拒否する条件として２通りあるが、第１の条件Ａ（アクセス拒否Ａ）では、上記①のアクセス要求に対してアクセス権限チェックを行なう。権限がない場合、アプリケーション２０２１が発行したＡＰＩの処理を行なわずに、結果としてアクセス違反のエラーを返す。

④第２の条件Ｂ（アクセス拒否Ｂ）では、②のアクセス要求に対してアクセス権限チェックを行なう。権限がなく、かつ、アプリケーション２０２１が発行し

たＡＰＩの結果としてエラーを返すことができない場合、アプリケーション２０２１が要求したリソースへの処理を行なわずに、リソース管理プログラム２０３が予め用意したダミーのリソースへのアクセス要求に代えて、ＡＰＩの処理を行なう。

その結果、アプリケーション２０２１は要求に成功したように動作するが、実際には要求したリソースにアクセスできない。

【００１６】

⑤アクセス要求①に対してアクセス権限チェックを行った結果、権限がある場合、ＡＰＩ監視ＣＴＲＬ２０３１がその要求を捕捉し、アプリケーション２０２１が発行したＡＰＩの処理をそのまま汎用ＯＳ２０１に伝え、その結果をアプリケーション２０２１に返す。

⑥上記⑤の処理によって、ＡＰＩが成功し、かつ、そのＡＰＩによってアプリケーション２０２１がリソースを保持する場合は、ＡＰＬ監視ＣＴＲＬ２０３２に伝える。ＡＰＬ監視ＣＴＲＬ２０３２はアプリケーション２０２１と保持しているリソースの対応を登録する。

アプリケーション２０２１がリソースの解放要求ＡＰＩを発行し、かつそのＡＰＩが成功した場合も、ＡＰＬ監視ＣＴＲＬ２０３２に伝える。ＡＰＬ監視ＣＴＲＬ２０３２はアプリケーション２０２１と保持していたリソースの対応を抹消する。

⑦ＯＳ標準機能の操作によって、リソースへのアクセス要求があれば、ＯＳ監視ＣＴＲＬ２０３４がその要求を捕捉し、アクセス制御ＣＴＲＬ２０３３に伝える。

⑧アクセス要求⑦に対してアクセス権限チェックを行なう。権限がない場合、⑦の操作を無視する。

⑨アクセス要求⑦に対してアクセス権限チェックを行なう。権限がある場合、⑦の操作を汎用ＯＳ２０１に伝える。

【００１７】

図４は、目的とするリソースに対するアクセス権限がある場合に、そのリソースを解放するまでのアプリケーション２０２１、リソース管理プログラム２０３

、汎用ＯＳ２０１のやり取りを示したＡＰＩの監視及び制御の第１の基本型（１）のシーケンス図である。

この第１の基本型（１）では、アプリケーション２０２１から目的のリソースへのアクセス要求があった場合（ステップ４０１）、リソース管理プログラム２０３はアクセス権があるかチェックし（ステップ４０２）、アクセス権がある場合（ステップ４０３）、汎用ＯＳ２０１にアプリケーション２０２１が発行したＡＰＩをそのまま伝える。汎用ＯＳ２０１は、ＯＳ本来のＡＰＩ処理を行なう（ステップ４０４）。

リソース管理プログラム２０３は、ＡＰＩが成功した場合、アプリケーション２０２１がそのリソースを保持しているという情報を登録する（ステップ４０５）。そして、汎用ＯＳ２０１からのＡＰＩ結果をそのままアプリケーション２０２１に返す（ステップ４０６）。これにより、リソースへのアクセス完了となる（ステップ４０７）。

【００１８】

この後、アプリケーション２０２１から保持しているリソースの解放要求が発行された場合（ステップ４０８）、リソース管理プログラム２０３はその解放要求を汎用ＯＳ２０１に伝える。汎用ＯＳ２０１は、ＯＳ本来のＡＰＩ処理を行なう（ステップ４０９）。リソース管理プログラム２０３は、ＡＰＩが成功した場合、アプリケーション２０２１がそのリソースを保持しているという情報を解除する（ステップ４１０）。そして、汎用ＯＳ２０１からのＡＰＩ結果をそのままアプリケーション２０２１返す（ステップ４１１）。これにより、保持しているリソースの解放完了となる（ステップ４１２）。

【００１９】

図５は、目的とするリソースに対するアクセス権限がなかった場合に、そのアクセスが拒否されるまでのアプリケーション２０２１、リソース管理プログラム２０３、汎用ＯＳ２０１のやり取りを示したＡＰＩの監視及び制御の第２の基本型（２）のシーケンス図である。

この第２の基本型（２）では、アプリケーション２０２１から目的のリソースへのアクセス要求があった場合（ステップ５０１）、リソース管理プログラム２

０３はアクセス権があるかチェックし（ステップ５０２）、アクセス権がなかった場合（ステップ５０３）、アクセス違反エラーをアプリケーション２０２１に返す（ステップ５０４）。これにより、リソースへのアクセス完了となる（ステップ５０５）。

また、アプリケーション２０２１がアクセス違反エラーに対応していないものにあっては、アプリケーション２０２１から目的のリソースへのアクセス要求があった場合（ステップ５０６）、リソース管理プログラム２０３はアクセス権があるかチェックし（ステップ５０７）、アクセス権がなく、かつ、アプリケーション２０２１がアクセス違反エラーに対応していない場合（ステップ５０８）、リソース管理プログラム２０３が予め用意したダミーのリソースへのアクセス要求に置き換え、汎用ＯＳ２０１に渡す（ステップ５０９）。

【００２０】

汎用ＯＳ２０１は、ＯＳ本来のＡＰＩ処理を行なう（ステップ５１０）。リソース管理プログラム２０３は、汎用ＯＳ２０１からのＡＰＩ結果をそのままアプリケーション２０２１返す（ステップ５１１）。この結果、目的のリソースへのアクセス完了となるが、ダミーリソースのため、実質的には何も行われない（ステップ５１２）。

【００２１】

本発明は、以上のようにしてアクセス権限のないリソースへのアクセスを制限するものであるが、汎用のＯＳであるＷｉｎｄｏｗｓとＵＮＩＸの場合のＡＰＩを例に挙げて説明する。

まず、ファイルへの複製を禁止する例について説明する。

ファイルへの複製については、従来、読み込み許可ファイルはファイルのコピーが可能であり、その結果オリジナルが複数存在したり、別媒体にて持ち出すことが可能であった。本発明では、ファイルコピーを実現するＡＰＩを監視／制御することにより、権限のないファイルのコピーを禁止する。その場合に、Ｗｉｎｄｏｗｓにおいて監視／制御するＡＰＩとして次のものがある。なお、以下で例示するＡＰＩの機能については、各種の文献で公開されているので、その詳細な説明は省略する。

（１）ファイルオープン／作成ＡＰＩ

ＣｒｅａｔｅＦｉｌｅＡ

ＣｒｅａｔｅＦｉｌｅＷ

ＯｐｅｎＦｉｌｅ

＿ｌｏｐｅｎ

＿ｌｃｒｅａｔ

ＧｅｔＯｐｅｎＦｉｌｅＮａｍｅＡ

ＧｅｔＯｐｅｎＦｉｌｅＮａｍｅＷ

ＧｅｔＳａｖｅＦｉｌｅＮａｍｅＡ

ＧｅｔＳａｖｅＦｉｌｅＮａｍｅＷ

（２）ファイルクローズＡＰＩ

ＣｌｏｓｅＨａｎｄｌｅ

＿ｌｃｌｏｓｅ

（３）ファイルコピー／移動ＡＰＩ

ＣｏｐｙＦｉｌｅＡ

ＣｏｐｙＦｉｌｅＷ

ＭｏｖｅＦｉｌｅＡ

ＭｏｖｅＦｉｌｅＷ

ＭｏｖｅＦｉｌｅＥｘＡ

ＭｏｖｅＦｉｌｅＥｘＷ

ＤｅｌｅｔｅＦｉｌｅＡ

ＤｅｌｅｔｅＦｉｌｅＷ

ＤｒａｇＱｕｅｒｙＦｉｌｅＡ

ＤｒａｇＱｕｅｒｙＦｉｌｅＷ

ＵＮＩＸの場合、監視／制御するＡＰＩとしては次のものがある。

（１）ファイルオープン／作成ＡＰＩ

ｏｐｅｎ

ｃｒｅａｔ

（２）ファイルクローズＡＰＩ

ｃｌｏｓｅ

（３）ファイルコピー／移動ＡＰＩ

ｒｅｎａｍｅ

【００２２】

このようなＡＰＩの監視によってファイルへの複製を禁止する場合、具体的な方法として３つの方法がある。

＜方法１＞（ファイルオープン中に複製処理を行なうことが判明している場合）

アプリケーションが、複製権限のないファイルをオープンし保持している間（ファイルをクローズするまでの期間）、そのアプリケーションが別のファイルを作成することを拒否する。

＜方法２＞（ファイルクローズ後に複製処理を行なう可能性はあるが、複数ファイルを扱わないことが判明している場合）

アプリケーションが、複製権限のないファイルを一度でもオープンした場合、そのアプリケーションが終了するか、複製権限のあるファイルをオープンするまで、そのアプリケーションが別のファイルを作成することを拒否する。

＜方法３＞（ファイルクローズ後に複製処理を行なう可能性があり、複数ファイルを扱う可能性がある場合）

アプリケーションが、複製権限のないファイルを一度でもオープンした場合、そのアプリケーションが終了するまで、そのアプリケーションが別のファイルを作成することを拒否する。

なお、いずれの方法であっても、別に作成されるファイルによって複製が残ることがないと判明している場合（一時ファイルなどの作成）は拒否しない。

【００２３】

次に、特定ファイルまたは全ての印刷を禁止する例について説明する。

従来、印刷機能を実装したアプリケーションによって、ファイルの内容を印刷し、外部に持ち出すことは可能であった。本発明では、印刷を実現するＡＰＩを監視／制御することにより、権限のないファイルの印刷を禁止する。またＦＡＸなどその他の外部出力装置についても、それぞれのデバイスを監視／制御すること

により、同様に禁止する。その場合に、Ｗｉｎｄｏｗｓ及びＵＮＩＸにおいて監視／制御するＡＰＩとして次のものがある。

Ｗｉｎｄｏｗｓの場合

（１）デバイスオープンＡＰＩ

ＣｒｅａｔｅＤＣＡ

ＣｒｅａｔｅＤＣＷ

（２）デバイスクローズＡＰＩ

ＲｅｌｅａｓｅＤＣ

ＣｌｏｓｅＰｒｉｎｔｅｒ

（３）プリンタ選択／ＡＰＬ処理ＡＰＩ

ＯｐｅｎＰｒｉｎｔｅｒＡ

ＯｐｅｎＰｒｉｎｔｅｒＷ

ＧｅｔＰｒｉｎｔｅｒＡ

ＧｅｔＰｒｉｎｔｅｒＷ

ＳｅｔＰｒｉｎｔｅｒＡ

ＳｅｔＰｒｉｎｔｅｒＷ

ＳｅｎｄＭｅｓｓａｇｅＡ

ＳｅｎｄＭｅｓｓａｇｅＷ

ＰｏｓｔＭｅｓｓａｇｅＡ

ＰｏｓｔＭｅｓｓａｇｅＷ

ＵＮＩＸの場合

（１）デバイスオープンＡＰＩ

ｏｐｅｎ

（２）デバイス制御ＡＰＩ

ｉｏｃｔｒｌ

（３）デバイスクローズＡＰＩ

ｃｌｏｓｅ

【００２４】

このようなＡＰＩの監視によって印刷を禁止する場合、具体的な方法として３

つの方法がある。

＜方法１＞（ファイルオープン中に印刷処理可能なことが判明している場合）

アプリケーションが、印刷権限のないファイルをオープンし保持している間（ファイルをクローズするまでの期間）、そのアプリケーションのプリンタ選択、およびプリンタデバイスのオープンを拒否する。

＜方法２＞（ファイルクローズ後に印刷処理を行なう可能性はあるが、複数ファイルを扱わないことが判明している場合）

アプリケーションが、印刷権限のないファイルを一度でもオープンした場合、そのアプリケーションが終了するか、印刷権限のあるファイルをオープンするまで、そのアプリケーションのプリンタ選択、およびプリンタデバイスのオープンを拒否する。

＜方法３＞（ファイルクローズ後に印刷処理を行なう可能性があり、複数ファイルを扱う可能性がある場合）

アプリケーションが、印刷権限のないファイルを一度でもオープンした場合、そのアプリケーションが終了するまで、そのアプリケーションのプリンタ選択、およびプリンタデバイスのオープンを拒否する。

【００２５】

次に、外部装置の利用を禁止する例について説明する。

従来、ＯＳに装備されている機能や外部装置そのものに権限を付加することは、一般的にはできなかった。本発明では、監視／制御すべきＡＰＩを限定できる機能の指定や、外部装置利用の指定をすることにより、その利用を禁止する。その場合に、Ｗｉｎｄｏｗｓ及びＵＮＩＸにおいて監視／制御するＡＰＩとして次のものがある。

Ｗｉｎｄｏｗｓの場合

（１）デバイスオープンＡＰＩ

ＣｒｅａｔｅＦｉｌｅＡ

ＣｒｅａｔｅＦｉｌｅＷ

ＯｐｅｎＦｉｌｅ

＿ｌｏｐｅｎ

＿ｌｃｒｅａｔ

（２）デバイスクローズＡＰＩ

ＣｌｏｓｅＨａｎｄｌｅ

＿ｌｃｌｏｓｅ

ＵＮＩＸの場合

（１）デバイスオープンＡＰＩ

ｏｐｅｎ

（２）デバイス制御ＡＰＩ

ｉｏｃｔｒｌ

（３）デバイスクローズＡＰＩ

ｃｌｏｓｅ

【００２６】

例えば、このようなＡＰＩの監視によって印刷を禁止する場合、具体的な方法として次の方法がある。

＜方法＞

アクセス権限テーブルにて、特定の条件のもとに特定デバイスの使用を禁止されている場合、そのデバイスの利用を以下の方法で拒否する。そのデバイスのデバイス名をもってデバイスオープンＡＰＩ要求があった場合、アクセス禁止エラー、もしくはデバイスが存在しないというエラーを返すことで要求を拒否する。

【００２７】

次に、ファイル内の一部のデータまたは全ての複写を禁止する例について説明する。

従来、アプリケーションによってファイルを画面表示した結果、その内容のすべてまたは一部をＯＳの機能によって複写またはオブジェクトという単位で別ファイルに埋め込むことが可能であった。

本発明では、転写や埋め込み機能を実現するＡＰＩ（クリップボードのＡＰＩ、ＯＬＥのＡＰＩなど）を監視／制御することで、権限のない流用を禁止する。その場合に、Ｗｉｎｄｏｗｓにおいて監視／制御するＡＰＩとして次のものがある。

Ｗｉｎｄｏｗｓの場合

（１）複写／埋め込みＡＰＩ

ＯｐｅｎＣｌｉｐｂｏａｒｄ

ＳｅｔＣｌｉｐｂｏａｒｄＤａｔａ

ＧｅｔＣｌｉｐｂｏａｒｄＤａｔａ

ＧｅｔＯｐｅｎＣｌｉｐｂｏａｒｄＷｉｎｄｏｗ

ＯｌｅＣｒｅａｔｅ

ＯｌｅＣｒｅａｔｅＥｘ

ＯｌｅＣｒｅａｔｅＦｒｏｍＦｉｌｅ

ＯｌｅＣｒｅａｔｅＦｒｏｍＦｉｌｅＥｘ

ＯｌｅＣｒｅａｔｅＦｒｏｍＤａｔａ

ＯｌｅＣｒｅａｔｅＦｒｏｍＤａｔａＥｘ

ＯｌｅＣｒｅａｔｅＬｉｎｋ

ＯｌｅＣｒｅａｔｅＬｉｎｋＥｘ

ＯｌｅＣｒｅａｔｅＬｉｎｋＦｒｏｍＤａｔａ

ＯｌｅＣｒｅａｔｅＬｉｎｋＦｒｏｍＤａｔａＥｘ

ＯｌｅＣｒｅａｔｅＬｉｎｋＴｏＦｉｌｅ

ＯｌｅＣｒｅａｔｅＬｉｎｋＴｏＦｉｌｅＥｘ

ＣｌｏｓｅＣｌｉｐｂｏａｒｄ

【００２８】

このようなＡＰＩの監視によって複写を禁止する場合、具体的な方法として４つの方法がある。

＜方法１＞（ファイルオープン中に複写処理可能なことが判明している場合）

アプリケーションが、複写権限のないファイルをオープンし保持している間（ファイルをクローズするまでの期間）、そのアプリケーションが複写／埋め込みオブジェクトの形式でデータを登録する際に、拒否もしくは空データを登録する。

＜方法２＞（ファイルクローズ後に複写処理を行なう可能性はあるが、複数ファイルを扱わないことが判明している場合）

アプリケーションが、複写権限のないファイルを一度でもオープンした場合、そのアプリケーションが終了するか、複写権限のあるファイルをオープンするまで、そのアプリケーションが複写／埋め込みオブジェクトの形式でデータを登録する際に、拒否もしくは空データを登録する。

＜方法３＞（ファイルクローズ後に複写処理を行なう可能性があり、複数ファイルを扱う可能性がある場合）

アプリケーションが、複写権限のないファイルを一度でもオープンした場合、そのアプリケーションが終了するまで、そのアプリケーションが複写／埋め込みオブジェクトの形式でデータを登録する際に、拒否もしくは空データを登録する。

＜方法４＞（複写権限のないファイルを埋め込みオブジェクトとして取り込む場合）

複写権限のないファイルを取り込む処理を行なう際に、オブジェクトの登録もしくはそのオブジェクトの取得ＡＰＩにおいて、アクセス違反のエラーを返すか、空データを登録あるいは取得することで、処理要求を拒否する。

【００２９】

次に、ネットワークを介してファイルが外部へ流出することを禁止する例について説明する。

従来、ファイルコピー以外に、ＦＴＰプログラムのように、ネットワークを介してファイルを外部へ転送することは可能であった。本発明では、ネットワークリソースにアクセスするＡＰＩを監視／制御することで、権限のないファイルを使用中のアプリケーションから外部への流出を禁止する。その場合に、Ｗｉｎｄｏｗｓ及びＵＮＩＸにおいて監視／制御するＡＰＩとして次のものがある。

Ｗｉｎｄｏｗｓの場合

ＷＳＡＳｔａｒｔｕｐ

ａｃｃｅｐｔ

ｂｉｎｄ

ｃｏｎｎｅｃｔ

ｇｅｔｈｏｓｔｂｙｎａｍｅ

ｇｅｔｈｏｓｔｂｙａｄｄｒ

ｇｅｔｐｒｏｔｏｂｙｎａｍｅ

ｇｅｔｐｒｏｔｏｂｙｎｕｍｂｅｒ

ｇｅｔｓｅｒｖｂｙｎａｍｅ

ｇｅｔｓｅｒｖｂｙｐｏｒｔ

ｇｅｔｐｅｅｒｎａｍｅ

ｇｅｔｓｏｃｋｎａｍｅ

ｇｅｔｈｏｓｔｎａｍｅ

ｇｅｔｓｏｃｋｏｐｔ

ｓｅｔｓｏｃｋｏｐｔ

ｒｅｃｖ

ｒｅｃｖｆｒｏｍ

ｓｏｃｋｅｔ

ｓｅｌｅｃｔ

ｓｅｎｄ

ｓｅｎｄｔｏ

ＷＳＡＳｅｎｄ

ＷＳＡＳｅｎｄＴｏ

ＷＳＡＡｓｙｎｃＳｅｌｅｃｔ

ＷＳＡＡｓｙｎｃＧｅｔＨｏｓｔＢｙＡｄｄｒ

ＷＳＡＡｓｙｎｃＧｅｔＨｏｓｔＢｙＮａｍｅ

ＷＳＡＡｓｙｎｃＧｅｔＰｒｏｔｏＢｙＮｕｍｂｅｒ

ＷＳＡＡｓｙｎｃＧｅｔＰｒｏｔｏＢｙＮａｍｅ

ＷＳＡＡｓｙｎｃＧｅｔＳｅｒｖＢｙＰｏｒｔ

ＷＳＡＡｓｙｎｃＧｅｔＳｅｒｖＢｙＮａｍｅ

ＷＳＡＣａｎｃｅｌＡｓｙｎｃＲｅｑｕｅｓｔ

ＷＳＡＳｅｔＢｌｏｃｋｉｎｇＨｏｏｋ

ＷＳＡＵｎｈｏｏｋＢｌｏｃｋｉｎｇＨｏｏｋ

ＷＳＡＣｌｅａｎｕｐ

ｃｌｏｓｅｓｏｃｋｅｔ

ｓｈｕｔｄｏｗｎ

ＵＮＩＸの場合

ａｃｃｅｐｔ

ｂｉｎｄ

ｃｏｎｎｅｃｔ

ｇｅｔｈｏｓｔｂｙｎａｍｅ

ｇｅｔｈｏｓｔｂｙａｄｄｒ

ｇｅｔｐｒｏｔｏｂｙｎａｍｅ

ｇｅｔｐｒｏｔｏｂｙｎｕｍｂｅｒ

ｇｅｔｓｅｒｖｂｙｎａｍｅ

ｇｅｔｓｅｒｖｂｙｐｏｒｔ

ｇｅｔｐｅｅｒｎａｍｅ

ｇｅｔｓｏｃｋｎａｍｅ

ｇｅｔｈｏｓｔｎａｍｅ

ｇｅｔｓｏｃｋｏｐｔ

ｓｅｔｓｏｃｋｏｐｔ

ｒｅｃｖ

ｒｅｃｖｆｒｏｍ

ｓｏｃｋｅｔ

ｓｅｌｅｃｔ

ｓｅｎｄ

ｓｅｎｄｔｏ

ｃｌｏｓｅｓｏｃｋｅｔ

ｓｈｕｔｄｏｗｎ

【００３０】

このようなＡＰＩの監視によって外部への流出を禁止する場合、具体的な方法として３つの方法がある。

＜方法１＞（ファイルオープン中に出力処理可能なことが判明している場合）

アプリケーションが、外部出力権限のないファイルをオープンし保持している間（ファイルをクローズするまでの期間）、そのアプリケーションからの接続要求や送信要求を、アクセス違反もしくはタイムアウトなどのエラーで拒否する。

＜方法２＞（ファイルクローズ後に出力処理を行なう可能性はあるが、複数ファイルを扱わないことが判明している場合）

アプリケーションが、出力権限のないファイルを一度でもオープンした場合、そのアプリケーションが終了するか、出力権限のあるファイルをオープンするまで、そのアプリケーションの接続要求や送信要求を、アクセス違反もしくはタイムアウトなどのエラーで拒否する。

＜方法３＞（ファイルクローズ後に出力処理を行なう可能性があり、複数ファイルを扱う可能性がある場合）

アプリケーションが、出力権限のないファイルを一度でもオープンした場合、そのアプリケーションが終了するまで、そのアプリケーションの接続要求や送信要求を、アクセス違反もしくはタイムアウトなどのエラーで拒否する。

ただし、その通信によってデータ出力されないことが判明している場合は、拒否しない。

【００３１】

次に、ファイルの内容のイメージを取得することを禁止する例について説明する。

ＯＳの機能として画面全体や一部、またはウインドウ単位のハードコピーをイメージデータとして取得することが、一般的には可能であり、従来、そのイメージデータを流用、持ち出しすることができた。本発明では、画面内のイメージデータ取得ＡＰＩを監視／制御することで、イメージデータ取得を禁止する。

その場合に、Ｗｉｎｄｏｗｓにおいて監視／制御するＡＰＩとして次のものがある。

（１）デバイスオープンＡＰＩ

ＧｅｔＷｉｎｄｏｗＤＣ

ＷｉｎｄｏｗＦｒｏｍＤＣ

ＧｅｔＤＣ

ＧｅｔＤＣＥＸ

ＧｅｔＤｅｓｋｔｏｐＷｉｎｄｏｗ

ＧｅｔＤｅｖｉｃｅＣａｐｓ

ＣｒｅａｔｅＤＣＡ

ＣｒｅａｔｅＤＣＷ

（２）イメージ取得ＡＰＩ

ＢｉｔＢｌｔ

ＳｔｒｅｔｃｈＢｌｔ

（３）デバイスクローズＡＰＩ

ＤｅｌｅｔｅＤＣ

ＲｅｌｅａｓｅＤＣ

【００３２】

このようなＡＰＩの監視によってイメージを取得することを禁止する場合、具体的な方法として３つの方法がある。

＜方法１＞（画面全体のハードコピーを拒否する場合）

現在画面上に表示されているウインドウを所有しているアプリケーションが、ハードコピー取得権限のないファイルを保持している場合、画面全体のハードコピー取得を拒否する。画面全体のハードコピーは、画面全体を管理しているウインドウ（Ｗｉｎｄｏｗｓの場合はデスクトップウインドウ）を監視することで、＜方法２＞と同じ。

ＷｉｎｄｏｗｓにおけるＤｉｒｅｃｔＤｒａｗなど、画面全体のハードコピーを取得するＡＰＩが存在すれば、同様に拒否する。

さらに、ディスプレイデバイスからＶＲＡＭイメージを取得するアプリケーションに対しては、それを拒否する。

＜方法２＞（ウインドウのハードコピーを拒否する場合）

現在画面上に表示されているウインドウを所有しているアプリケーションが、ハードコピー取得権限のないファイルを保持している場合、そのウインドウのハードコピー取得を拒否する。ウインドウが画面上に表示されているかは、ウインドウの状態を監視することで行なう。

また、ハードコピー取得の拒否は、そのウインドウに関連付けられたデバイスコンテキストからのイメージコピーを拒否することで行なう。

＜方法３＞（画面の一部のハードコピーを拒否する場合）

ハードコピーを取得する領域が判断できる場合は、＜方法１＞における条件を、取得領域が対象となるウインドウと重なる時とし、以降は＜方法１＞と同じ。また領域が判断できない時は、＜方法１＞と同じ。

【００３３】

次に、ファイル種別毎に利用アプリケーションを限定する例について説明する。

従来、アプリケーション利用に制限がないため、参照以外の目的でファイルにアクセス可能であった。本発明では、ファイルごとに利用アプリケーションを限定できる。その場合に、Ｗｉｎｄｏｗｓにおいて監視／制御するＡＰＩとして次のものがある。

（１）ファイルオープンＡＰＩ

ＣｒｅａｔｅＦｉｌｅＡ

ＣｒｅａｔｅＦｉｌｅＷ

ＯｐｅｎＦｉｌｅ

＿ｌｏｐｅｎ

＿ｌｃｒｅａｔ

（２）ファイルクローズＡＰＩ

ＣｌｏｓｅＨａｎｄｌｅ

＿ｌｃｌｏｓｅ

（３）プロセス管理ＡＰＩ

ＷｉｎＥｘｅｃ

ＣｒｅａｔｅＰｒｏｃｅｓｓＡ

ＣｒｅａｔｅＰｒｏｃｅｓｓＷ

ＥｘｉｔＰｒｏｃｅｓｓ

ＵＮＩＸの場合

（１）ファイルオープンＡＰＩ

ｏｐｅｎ

（２）ファイルクローズＡＰＩ

ｃｌｏｓｅ

【００３４】

このようなＡＰＩの監視によって利用アプリケーションを限定する場合、具体的な方法として次の方法がある。

＜方法＞

アプリケーションがファイルをオープンする際、そのファイルの権限をチェックし、許可されたアプリケーションでない場合はアクセス違反エラーを返すことで、オープン要求を拒否する。

次に、ＯＳの特定の機能の利用を禁止する例について説明する。

従来、ＯＳに装備されている機能に権限を付加することは、一般的にはできなかった。本発明では、監視／制御すべきＡＰＩを限定する機能を指定することで、その利用を禁止することができる。例えば、ファイルのタイムスタンプやシステム日時の変更を禁止するなどである。その場合に、Ｗｉｎｄｏｗｓにおいて監視／制御するＡＰＩとして次のものがある。

（１）ファイルのタイムスタンプ変更ＡＰＩ

ＳｅｔＦｉｌｅＴｉｍｅ

（２）システム日時の変更ＡＰＩ

ＳｅｔＳｙｓｔｅｍＴｉｍｅ

ＳｅｔＳｙｓｔｅｍＴｉｍｅＡｄｊｕｓｔｍｅｎｔ

【００３５】

このようなＡＰＩの監視によってＯＳにおける特定の機能の利用を禁止する場合、具体的な方法として次の方法がある。

＜方法＞

特定の条件下で禁止されているＡＰＩが発行された際に、アクセス違反エラーを返すか、実際の処理を行なわずに（ダミー処理）正常リターンすることで、禁止されているＡＰＩ（ＯＳ機能）を拒否する。

【００３６】

次に、プロセス内メモリの参照または変更を禁止する例について説明する。

従来、アプリケーションが明示的に拒否しない限り、プロセス内メモリの参照／変更を禁止することができなかった。本発明では、プロセス内メモリの参照／変更ＡＰＩを監視／制御することで、他のアプリケーションからの参照／変更を禁止することができる。

その場合に、Ｗｉｎｄｏｗｓにおいて監視／制御するＡＰＩとして次のものがある。

（１）プロセス管理ＡＰＩ

ＯｐｅｎＰｒｏｃｅｓｓ

ＣｒｅａｔｅＰｒｏｃｅｓｓ

ＣｌｏｓｅＨａｎｄｌｅ

（２）メモリ操作ＡＰＩ

ＲｅａｄＰｒｏｃｅｓｓＭｅｍｏｒｙ

ＷｒｉｔｅＰｒｏｃｅｓｓＭｅｍｏｒｙ

ＲｅａｄＰｒｏｃｅｓｓＭｅｍｏｒｙＶｌｍ

ＷｒｉｔｅＰｒｏｃｅｓｓＭｅｍｏｒｙＶｌｍ

【００３７】

このようなＡＰＩの監視によってプロセス内メモリの参照または変更を禁止する印刷を禁止する場合、具体的な方法として次の方法がある。

＜方法＞

アクセスが禁止されているアプリケーションのプロセス内メモリにおいて、メモリ操作ＡＰＩが要求された際に、アクセス違反エラーを返す。

次に、ブラウザに表示したＷｅｂページの印刷や保存や外部装置への出力を禁止する例について説明する。

従来、閲覧や再生のみを許可したＷｅｂページでも、実際にはブラウザソフトによって印刷や保存が可能であった。ＷｅｂページをロードするためのネットワークリソースにアクセスするＡＰＩを監視し、ブラウザが行う印刷や保存のアプリケーションを監視／制御することにより、印刷や保存や外部装置への出力操作を禁止することができる。その場合に、監視／制御するＡＰＩとして次のような

ものがある。

Ｗｉｎｄｏｗｓの場合

（１）通信ＡＰＩ

ＷＳＡＳｔａｒｔｕｐ

ａｃｃｅｐｔ

ｂｉｎｄ

ｃｏｎｎｅｃｔ

ｇｅｔｈｏｓｔｂｙｎａｍｅ

ｇｅｔｈｏｓｔｂｙａｄｄｒ

ｇｅｔｐｒｏｔｏｂｙｎａｍｅ

ｇｅｔｐｒｏｔｏｂｙｎｕｍｂｅｒ

ｇｅｔｓｅｒｖｂｙｎａｍｅ

ｇｅｔｓｅｒｖｂｙｐｏｒｔ

ｇｅｔｐｅｅｒｎａｍｅ

ｇｅｔｓｏｃｋｎａｍｅ

ｇｅｔｈｏｓｔｎａｍｅ

ｇｅｔｓｏｃｋｏｐｔ

ｓｅｔｓｏｃｋｏｐｔ

ｒｅｃｖ

ｒｅｃｖｆｒｏｍ

ｓｏｃｋｅｔ

ｓｅｌｅｃｔ

ｓｅｎｄ

ｓｅｎｄｔｏ

ＷＳＡＳｅｎｄ

ＷＳＡＳｅｎｄＴｏ

ＷＳＡＡｓｙｎｃＳｅｌｅｃｔ

ＷＳＡＡｓｙｎｃＧｅｔＨｏｓｔＢｙＡｄｄｒ

ＷＳＡＡｓｙｎｃＧｅｔＨｏｓｔＢｙＮａｍｅ

ＷＳＡＡｓｙｎｃＧｅｔＰｒｏｔｏＢｙＮｕｍｂｅｒ

ＷＳＡＡｓｙｎｃＧｅｔＰｒｏｔｏＢｙＮａｍｅ

ＷＳＡＡｓｙｎｃＧｅｔＳｅｒｖＢｙＰｏｒｔ

ＷＳＡＡｓｙｎｃＧｅｔＳｅｒｖＢｙＮａｍｅ

ＷＳＡＣａｎｃｅｌＡｓｙｎｃＲｅｑｕｅｓｔ

ＷＳＡＳｅｔＢｌｏｃｋｉｎｇＨｏｏｋ

ＷＳＡＵｎｈｏｏｋＢｌｏｃｋｉｎｇＨｏｏｋ

ＷＳＡＣｌｅａｎｕｐ

ｃｌｏｓｅｓｏｃｋｅｔ

ｓｈｕｔｄｏｗｎ

（２）その他、前述のファイル、印刷、外部装置への操作を禁止する場合のＡＰＩ

ＵＮＩＸの場合

（１）

ａｃｃｅｐｔ

ｂｉｎｄ

ｃｏｎｎｅｃｔ

ｇｅｔｈｏｓｔｂｙｎａｍｅ

ｇｅｔｈｏｓｔｂｙａｄｄｒ

ｇｅｔｐｒｏｔｏｂｙｎａｍｅ

ｇｅｔｐｒｏｔｏｂｙｎｕｍｂｅｒ

ｇｅｔｓｅｒｖｂｙｎａｍｅ

ｇｅｔｓｅｒｖｂｙｐｏｒｔ

ｇｅｔｐｅｅｒｎａｍｅ

ｇｅｔｓｏｃｋｎａｍｅ

ｇｅｔｈｏｓｔｎａｍｅ

ｇｅｔｓｏｃｋｏｐｔ

ｓｅｔｓｏｃｋｏｐｔ

ｒｅｃｖ

ｒｅｃｖｆｒｏｍ

ｓｏｃｋｅｔ

ｓｅｌｅｃｔ

ｓｅｎｄ

ｓｅｎｄｔｏ

ｃｌｏｓｅｓｏｃｋｅｔ

ｓｈｕｔｄｏｗｎ

（２）その他、前述のファイル、印刷、外部装置への操作を禁止する場合のＡＰＩ

【００３８】

このような通信ＡＰＩを監視し、印刷や保存や外部装置への出力を禁止する方法として、次の方法がある。

まず、Ｗｅｂページ内に記述された禁止指定を読み取る。具体的には、ｈｔｔｐプロトコルまたは同等のプロトコルのデータを監視し、その中のＷｅｂページデータ部分に印刷や保存の禁止指定タグが含まれていれば、そのＷｅｂページは印刷や保存が禁止されていると判断する。または、権限の獲得を利用者に求め、獲得できなかった場合に印刷や保存が禁止されていると判断する。しかし、獲得できた場合には、印刷や保存が禁止されていないものと判断する。すなわち、アクセス権限が獲得できたか否かをもって、アクセス権限があるか否かを判定する。

印刷や保存や外部装置への出力が禁止されているページを表示しているブラウザが、印刷や保存を行なおうとした場合、前述した印刷やファイルの保存や外部装置への出力を禁止する方法を用いて、それを禁止する。

ここで説明したＷｅｂページの例は、そのしくみの類似性により、容易にディジタルテレビジョンのコンテンツにおいても利用できるものである。

【００３９】

次に、リソース管理プログラムを応用した例を示しておく。

図６は、リソース管理プログラム２０３が管理しているリソースのアクセス状況を履歴管理プログラム６０１に転送し、履歴管理データベース（ＤＢ）６０２

に格納しておき、必要に応じて、図８に示すようなアクセス監視履歴として画面表示する構成を示したものである。通報プログラム６０３は、不正なアクセスがあった場合にシステム管理者の端末に対し、図７（ｂ）で示すような内容の不正アクセス通知画面を送信し、表示させるものである。

なお、一般ユーザが不正アクセスを行なった場合には、図７（ａ）で示すような画面表示が行われる。

【００４０】

なお、上記の説明においては、アクセス権管理テーブルを参照してアクセス権限の有無を判定するようにしているが、コンピュータリソース内部に記述された、既存環境で定義されていない拡張したアクセス権を指定するアクセス権限情報を参照し、アクセス権限があるか否かを判定するようにすることもできる。

また、上記の説明において用いたネットワークリソースとは、通信媒体、デバイス、アクセスポイント、ディジタルテレビジョンのチャンネル、通信データまたはコンテンツなど、ＯＳが管理しているリソースのうちネットワークに関するものである。

【００４１】

以上のように、本実施形態においては、基本的には、ファイル、ネットワーク、記憶装置、表示画面、外部付属装置等のオペレーティングシステムが管理しているコンピュータリソースに対するプロセスまたはオペレーティングシステムからの操作要求をコンピュータリソースにアクセスする前に捕捉し、その捕捉した操作要求によって指定されるコンピュータリソースに対するアクセス権限があるか否かを判定し、アクセス権限があれば当該操作要求通りにオペレーティングシステムに渡し、その結果を要求元プロセスに返し、アクセス権限がなければ当該操作要求を拒否するようにしたため、ＯＳやプロセス（ＯＳの元に稼動しているプログラムであり、アプリケーションやデーモンなど）を変更することなく、ファイルや画面以外のコンピュータリソースを含めてアクセス権限のないユーザに対するリソースの操作を制限することができる。

また、リソース管理プログラムを既存の環境に組み込むだけで、上述したような各種の不正アクセスを制限することができ、既存のアクセス権の範囲を拡張す

ることが可能になる。

【００４２】

さらに、要求元のアプリケーションがアクセス違反に対応する機能を有していない場合であっても、ダミーのコンピュータリソースへの操作要求に変換してオペレーティングシステムに渡すようにしたため、アクセス違反に対応する機能を有していないアプリケーションに対しても対応することができる。

【００４３】

なお、リソース管理プログラムは、ＣＤ－ＲＯＭ等のディスク型ストレージ、半導体メモリ及び通信ネットワークなどの各種の媒体を通じてコンピュータにインストールまたはロードすることができる。また、プログラム製品単体として、コンピュータユーザに提供することができる。

また、実施形態で例示したＡＰＩについては、その一例を示しただけであって、ＯＳのバージョンアップなどによって追加された場合でも容易に対応できることは言うまでもない。

【００４４】

【第２実施形態】

図１０は本発明による第２の実施形態をしめす。図１０の１１は、先に説明したセキュリテイ環境における本発明のコンピュータアーキテクチャの構造を示す。本構成は、ハミングヘッズセキュリテイ管理方式（ＨＨシステム）の全体構成を示すもので、本発明による、コンピュータアーキテクチャのＨｉｅｒａｒｃｈｙを示した。

【００４５】

１７はＯＳで先に説明したようにＷｉｎｄｏｗｓでも、ＭＡＣでもＯＳはどれでもよい。ＯＳに依存しないのが特徴である。１８のＡＰＩ１（Ａｐｐｌｉｃａｔｉｏｎ　Ｐｒｏｇｒａｍ　Ｉｎｔｅｒｆａｃｅ　１）は、ＯＳの中に位置していて、ＯＳとのインターフェースの役割を果たす。１９のＳＣＭからの要求に応じて、ＯＳに指示をおくる。

この場合の指示とは、クライアントへの情報の提供の方法に関するものであって、情報を一切拒否したり、閲覧のみ可としたり、コピー、メール、転送等の許

可を行う。

【００４６】

１９のＳＣＭ（Ｓｅｃｕｒｉｔｙ　Ｃｏｎｔｒｏｌ　Ｍａｎａｇｅｍｅｎｔ）は、本発明の主旨であってＨ．Ｈ（ハミングヘッズ）セキュリテイモジュールを示す。

ＯＳ、ＡＰＬ（アプリケーション・ソフトウエア）の処理を監視している。

何らかの条件で、許可、不許可を決める。１２の管理テーブルがあって、本システムにどのような形でクライアントがアクセス可能か、クライアントがアクセスした場合、管理テーブルの中に人の名、電話番号、あるいはＩＤ番号でアクセスしたクライアントの位置付けと重みを判断する。

【００４７】

クライアントの要求をそのまま受け入れるか、条件をつけて許可するかは、１２に格納されているクライアントの個人データによって判断する。

情報の提供を要求どうりクライアントに提供できないが、課金する事によって提供できる事もある。図１１にＳＣＭ１９の位置付けの模式図を示している。

【００４８】

図１０の２０のＡＰＩ２（Ａｐｐｌｉｃａｔｉｏｎ　Ｐｒｏｇｒａｍ　Ｉｎｔｅｒｆａｃｅ　２）は、クライアントのアクセスを監視していて、アクセスがあればＯＳにわたす。

ＯＳのコントロール下にある外部デバイスの監視もおこなう。ＯＳの要求する全てのリソースが対象になる。

【００４９】

１４のファイルは、２０のＡＰＩ２に接続されていて、クライアントからのアクセス、要求の履歴を記憶する。

【００５０】

２１のＡＰＬは各種のアプリケーションプログラムであって、例えばマイクロソフト社のＯｆｆｉｃｅ２０００、Ｗｏｒｄ、Ｅｘｃｅｌ、Ｐｏｗｅｒ　Ｐｏｉｎｔなどの類である。クライアント、ユーザは文章、図、あるいは静止画、動画、音声、音楽等のＯＳのコントロール下で行う。１３は２１のファイルで各種の

アプリケーションソフト、クライアント、ユーザの作成した創作物を格納する。

【００５１】

図１０の２２は本サーバ、サイトと外部デバイスとを接続するインターフェースで、本例では、通信ネットワーク１５、ドライバーソフト１６を介してクライアント、ユーザの画面２３、プリンター２４、Ｆａｘ／コピー機２５に接続している。

又、クライアント、ユーザは通信ネットワーク１５を介して、ＰＣ等を接続して２３、２４、２５等のデバイスを用いて情報の提供を受けることが出来る。

【００５２】

図１０の２６は、公衆網通信インターフェース、２７は外部装置接続用のＵＳＢ、ＲＳ２３２Ｃ、ＩＥＥＥ１３９４等のシリアル、パラレルのコネクターと接続するラインである。２９は外部接続機器との接続線であって、１６のドライバソフトは、外部機器２３、２４、２５、２８か１１に内蔵されているのが一般的である。

【００５３】

図１１は、ＯＳ、外部装置、情報を格納してあるファイルと本発明によるＳＣＭとの関係を示した模式図である。ユーザ、クライアントによって作られた創作物、Ｈ．Ｈサイト（ハミングヘッズサイト）、サーバから提供される各種の情報は１３に格納してある。

この情報とは、文章、図、絵、音声、静止画、動画等を含む。

【００５４】

ＳＣＭ１９はＯＳ１７とＡＰＬ２１の中間に位置して情報の抽出、使用について、クライアント、ユーザの動きを監視している。ＯＳのコントロール下で外部装置２３、２４、２５、２８への情報の出力についてクライアント、ユーザの権限をチェックして、制限をくわえる。制限とは、先に説明したように情報のコピー、メール、転送の許諾権を与えるものである。

【００５５】

ＳＣＭ１９に接続しているファイル１２には、クライアント、ユーザの権限情報を格納していて、要求に応じてその都度、照合して外部装置、デバイスへの出

力に制限をくわえる。クライアント、ユーザはあらかじめ個人の情報を登録しておく必要がある。企業、法人、政府機関、自治体等であれば、部長、課長、一般職というように職位によって権限を制限したり、与えたりしてもよい。

【００５６】

又、外部の一般人がクライアント、ユーザとしてアクセス要求がある場合もある。その時には、外部に出せる情報であれば無料のものと有料のものとを層別してＳＣＭ１９が管理しておけばよい。

【００５７】

【第３実施形態】

図１２は第３の実施形態を示すシステム構成図である。通信ネットワーク１５は、公衆網でＩＮＮＴアーネットＩＰ、電話網ＰＳＴＮ、ＸＤＳＬ網、デジタル網ＩＳＤＮ、Ｂ－ＩＳＤＮ、ＡＴＭ、モバイル網、衛星網等を使用している。

３１は公式のＷｅｂサイトで例えばＮＴＴドコモ社のｉモードのサイトがある。３２はモバイル無線網のアンテナで、本実施例ではｉモードサイトに接続している。もちろんＰＨＳ、他のＰＤＣ（Ｐｅｒｓｏｎａｌ　Ｄｅｇｉｔａｌ　Ｃｅｌｌａｒ）も使用できる。特にＩＭＴ２０００は高速なので動画の伝送に優れている。

【００５８】

３３は本発明によるＨ．Ｈサイトで情報提供を行う。先に説明したようにセキュリテイを万全にしたシステムであって、ユーザ、クライアントの権限によって制限を設けるものである。Ｈ．ＨサイトはＳＣＭ１９をインプリメントしたソフトを搭載したサーバを使用している。

【００５９】

３４はデータベースのサイトであって各種のビジネス、研究等に必要な情報が格納してあって、Ｈ．Ｈサイトを介して使用できる。３５はＷｅｂキャストでデジタル放送をＨ．Ｈサイトを通して利用できる。３６は金融機関のサイトでＨ．Ｈサイトを使用して課金された場合、使用料の徴収をおこなう。

【００６０】

３７はＷｅｂ上に設けられたモールで、Ｈ．Ｈサイトを通してショッピングが

できる。購入の支払いは３６の金融機関のサイトよりおこなう。

Ｗｅｂ上で商品を買ったり、デジタル放送を見たり聞いたりして、課金が発生したときにはＨ．Ｈサイトを介しているので、利用者であるクライアント、ユーザそれにサービスの提供者はセキュリテイが万全であるから安心して使用できる。

【００６１】

図１２の３８は利用者のための端末機器をコンビニ、街角、広場に設置した例である。図示してないがプリンター、コピー機等も接続している。

３９は学校、研究機関を、４０は工場、オフィスを示す。

４１は一般家庭での使用例で４５は、ホームサーバを示す。近年、在宅で仕事をする人がふえてきた。通信回線の発展の恩恵によるものであって、企業内のデータ、情報を活用する場合本発明によるセキュリテイの効果が発揮する。４６はホームルータである。

【００６２】

図１２の４２は携帯情報端末機器でモバイル機器ともいう。携帯電話機の普及は顕著で、特にｉモードの発展は急速にたちあがった。ＣＨＴＭＬのブラウザにメールが可能で、これをもってＨ．Ｈサイトにもアクセスできるから利便性はよい。さらにＰａｌｍＯＳに見られるようにＰＤＡ（携帯情報機器）の使い勝手もよい。プリンター、インターネットカメラ、デジタルカメラを搭載したり接続もできる。

【００６３】

４３はクライアント、ユーザである。図１２ではモバイラーとして４３の人は場所を問わず、何処ででも仕事ができる。当然Ｈ．Ｈのセキュリテイである権限制限機能が発揮されるから、図示してない企業のイントラネットも容易に使用できる。

【００６４】

４４は車載移動体で、モバイルインターネットによって同様にＨ．Ｈサイトからのサービスを受けることができる。先に説明したようにＨ．Ｈサイトをはじめ、Ｈ．Ｈサーバも図１１の１９のＳＣＭの機能によって安全に情報の管理が出来

る。

【００６５】

【第４実施形態】

図１３は第４の実施形態をしめす。企業内のイントラネットに本発明を応用した例である。配信ネットワーク１５より２６の回線を介してルータ５１に接続されている。５２はＷＷＷサーバで５３はファイアウオールである。５３を介して本セキュリテイを搭載したサーバ５５に接続される。５５はＨ．Ｈサーバである

【００６６】

５６は５５とＬＡＮ５４で接続されている企業のデータベースである。このデータベースには、顧客のリスト、営業情報、工場であれば生産、製造の技術情報、設計開発の情報等企業活動に必要な各種のデータ、情報が格納されていてクライアントである企業の社員は先に説明したような、権限に応じて制限して利用できる。職能階層に応じて利用できる情報とできない情報がある。場合によっては代表権のある役員しか開示できない情報もあって、５５のサーバに搭載されたＨ．Ｈ方式によって管理されている。

【００６７】

企業内ＬＡＮ５４を介して接続してある５７、５８、５９ｍｎは、企業内のクライアントＰＣ、サーバである。５９は多機能電話機、６０はプリンター、ＦＡＸ／コピー機である。６１は携帯情報端末機器、ＰＤＡを６２は携帯電話機６３はモバイルノートＰＣを示す。これらの機器は社内、構内モバイル機器として用いる。６５は構内移動車載端末を示す。

６４は企業内、構内モバイル端末機器用のアンテナを示す。

【００６８】

本イントラネットは、企業だけでなく法人、研究機関、教育機関でも使用できるのをはじめ、企業外からもアクセスできる。外からの使用はセキュリテイを確保して内部の情報を出すことが可能になる。本発明によるシステムはきわめて有効である。

【００６９】

【第５実施形態】

図１４は第５の実施形態をしめす。ホームでの実施例を示す。先に説明したようにＩＴの普及によって、家庭で就労する人が増えてきた。我が国でもすでに６百万人を超えたと言われている。少子高齢化と伴にこの傾向は増加の一途にあるといえる。

【００７０】

図１４において、２６の公衆回線よりホームルータ７２に接続される。１５はここでは公式Ｗｅｂサイトに接続している。例として、ＮＴＴドコモ社のｉモードサイトがある。７２のルータはホームＬＡＮ７３に接続されている。７３は有線ＬＡＮだけではなく、ブルートース、Ｉｒｄａを使用した無線ＬＡＮでもよい。７４はＰＣまたはホームサーバ、７５は大画面付きの多機能電話機、７６はＴＶ、７７は音響ＡＶ機器、７８はモバイル携帯情報端末機器を示す。７１はアンテナで公衆無線網との接続を行う。４１は家、家庭を示す。

【００７１】

在宅就労は各種の企業情報、機密情報を扱うのでセキュリテイの確保は最重要課題である。公式Ｗｅｂサイト３１を介して３３のＨ．Ｈサイトを通して情報の授受を行うから安全である。又、仕事だけでなく娯楽としてのコンテンツをネットワークから配信を受ける環境になってきた。３５のＷｅｂキャストからＴＶや音楽の配信を受けて、７６のＴＶ端末、７７のＡＶ機器、７８の家庭内モバイル端末で楽しんで、生活を豊かにすることができる。

【００７２】

娯楽コンテンツをネットワーク上のサイトから提供を受けた場合、料金の支払いが生ずる。３３のサイトで管理されているからクレジットカード番号を入力して３６の金融機関のサイトから自動引き落としが可能になる。この場合、なりすましを防止するために個人認証が必要になる。個人認証の方法は各種提案されているが、ＩＤ番号、電話番号のほかに機密度の高い場合は公開鍵を使用するのもよい。なお、７４のホームサーバに本発明のＳＣＭを搭載して安全を確保してもよい。組織に属して家庭で就労する場合、７４のサーバは企業から提供されたものを使用して家庭就労するという、条件を設けるのも一つのホームワーキングの

方法である。

【００７３】

図１５は本発明によるセキュリテイ確保についての流れ、ユーザ、クライアントに制限と課金を課すことを説明するフロー図である。

Ｓ８１はユーザ、クライアントが情報を得るためにサイトにアクセスする。Ｓ８２はH．Hサイト、H．HサーバにあるＳＣＭによってアクセスしてきたクライアント、ユーザの個人情報を検索、照合する。

【００７４】

Ｓ８３はクライアント、ユーザからの情報の特定を行う。ここでいう特定とは、機密度の程度と、アクセスしてきたクライアントの職位の階層によって権限の制限を受けるのが特徴である。クライアント、ユーザは組織に所属しているものであれば、職位の階層は自動判別できる。一般からのアクセスも可能であるから提供できる情報と出来ないものを区別する。また無料で提供できる企業のカタログ類とか宣伝類のほかに有料で頒布できる情報もある。有料でも価値の高いものは、課金の程度を変えて頒布するのを特徴とすれば、本H．Hサイトはビジネスとして成立する。

【００７５】

Ｓ８４ではH．Hサーバまたはサイトにアクセスして来た、クライアント、ユーザからの要求にこたえられるか、ＳＣＭにある個人情報と照合して判定する。

【００７６】

Ｓ８５では判定の結果、そのクライアントは情報を提供しても良い人であった。従ってＯＫの返事、表示を出す。次にＳ８６では、要求情報のコピーとメールで他人への転送の可否を聞いて来た。Ｓ８７ではクライアントの職責、権限をＳＣＭによってチェックする。先に説明したが、本発明では個人の権限によって情報の利用を制限するものである。

【００７７】

Ｓ８８ではコピーもメール転送もＯＫと判定された。このクライアントは、高位な権限をもっているか、要求情報の機密性の低いものであったと判断される。

Ｓ８９では、クライアント、ユーザの誰それがどんな情報、ドキュメントをい

つ、コピーしたか、メール転送したかの履歴がＨ．Ｈサーバ、サイトに記録される。

【００７８】

Ｓ９０はＨ．Ｈサーバ、サイトでの履歴の管理も終わり、情報、ドキュメントの提供する体制が整った。クライアントへ情報を提供する。

【００７９】

Ｓ９１ではアクセスして来たクライアントの要求がＳ８４の判定によって拒された。Ｓ９２ではクライアントはＩＤ番号を、もし初めてアクセスして来た人とか一般の人であれば身分を証明する、電話番号、保険証の番号、免許証、年金番号等を入力する。

【００８０】

お金を払えば提供できる情報もある。課金の金額をクライアントに知らせる。金額は情報、ドキュメントの機密度、重要度によって価値は変わる。従って金額も異なる。

Ｓ９３では課金されてもＨ．Ｈサーバ、サイトの方で提供できない情報もある。又、クライアントの方でも課金されたら不要であったり、課金の金額によっては入手したいという人もいる。いずれにしても、入手の許可があればＳ８５へ進む。なければこの処理を終了する。

【００８１】

Ｓ９４では、欲しい情報、ドキュメントのコピー、メール転送がＳ８７の判定によって不可と判定された。クライアント、ユーザへ画面で見ることは、許可されている。見るだけの情報がクライアントに送られるが、ＳＣＭ１９によってＯＳをコントロールしているからクライアントの端末に表示されていても、コピーとメールの転送はできない。

【００８２】

Ｓ９５ではＨ．Ｈサーバ、サイトに先に説明したような履歴を管理する。Ｓ９６ではクライアントの画面に要求のあった情報が表示される。どうしてもコピー、メール転送したい情報もある。ここであらためてサイト、サーバに許可の要求をだす。Ｓ９７では、課金して情報の入手を申請する。ここのステップではクラ

イアントの職責、階層は、Ｈ．Ｈサーバ、サイトに認知されているから金額の程度によって、許可できる場合もある。

【００８３】

課金すれば提供できるとサイト、サーバが判断した場合、金額を提示する。課金しても提供できないとサイト、サーバが判断すればこの処理はクライアントへの画面表示Ｓ９８のみで終了する。情報、ドキュメントの程度に応じて表示時間に制限を加えてもよい。所定時間内の表示を行って、より長時間見たい場合は課金制度を導入するのも一方法である。

【００８４】

この場合、Ｓ９９、Ｓ１００でＨ．Ｈサイト、サーバからより長時間の表示と課金の有無をクライアント、ユーザに問い合わせる。Ｈ．Ｈサーバ、サイトとクライアントが了解すればＳ１０１で画面表示を長時間行う。

【００８５】

Ｈ．Ｈサーバ、サイトの課金とクライアント、ユーザの了解が得られない場合は所定時間のみの表示Ｓ９８でこの処理は終了する。

【００８６】

以上説明したように、第１実施形態ではアクセス権限をＯＳやそのプロセスを変更しないでユーザ、クライアントに対して制限して不正行為を防止する例を、第２実施形態では、Ｈ．Ｈサイト、サーバのシステム構成を、第３実施形態では通信ネットワーク、特にインターネットを中心にして社会環境で発揮するＨ．Ｈサイトのシステム構成をしめす。

【００８７】

第４実施形態では企業内、工場、学校、研究機関、団体等のイントラネットに本Ｈ．Ｈサーバの応用について示し、第５実施形態では、ホームオフイス、在宅就労における本Ｈ．Ｈサイトの応用について示した。

【００８８】

なお、図１５のフロー図はＨ．Ｈサーバ、サイトを介して情報、ドキュメントの閲覧、コピーメール転送について説明してあるが、図１２のＷｅｂキャストからのデジタル放送の配信、各種無料有料コンテンツからの配信による課金システ

ムにも適用する。

【００８９】

【発明の効果】

以上の説明から明らかなように、本発明は、基本的には、ファイル、ネットワーク、記憶装置、表示画面、外部付属装置等のオペレーティングシステムが管理しているコンピュータリソースに対するプロセスまたはオペレーティングシステムからの操作要求をコンピュータリソースにアクセスする前に捕捉し、その捕捉した操作要求によって指定されるコンピュータリソースに対するアクセス権限があるか否かを判定し、アクセス権限があれば当該操作要求通りにオペレーティングシステムに渡し、その結果を要求元プロセスに返し、アクセス権限がなければ当該操作要求を拒否するようにしたため、ＯＳやプロセス（ＯＳの元に稼動しているプログラムであり、アプリケーションやデーモンなど）を変更することなく、ファイルや画面以外のコンピュータリソースを含めてアクセス権限のないユーザに対するリソースの操作を制限することができる。

また、リソース管理プログラムを既存の環境に組み込むだけで、上述したような各種の不正アクセスを制限することができ、既存のアクセス権の範囲を拡張することが可能になる。

また、リソース制御プログラムを既存の環境に組み込むだけで、各種の不正アクセスを制限することができ、従来のアクセス権の範囲を拡張することが可能になる。

さらに、アクセス違反に対応する機能を有していないアプリケーションに対しても対応することができるなどの効果が得られる。

【００９０】

急速に進展しているｅビジネスに本発明による権限制限システムを応用すれば、不正アクセスの防止、各種有料コンテンツの配信による課金に効力を発揮する。急激な高齢化社会の到来と伴に在宅就労も重要な課題になってきた。

本Ｈ．Ｈシステムの導入によって、安全に企業のドキュメント、データ、情報が家庭内で取り出せて、家庭内作業と成果をＷｅｂサイト、企業に送る事も可能になった。

【図面の簡単な説明】

【図１】

本発明の実施環境の第１実施形態を示すハードウェア構成図である。

【図２】

本発明に係るリソース管理プログラムの機能構成及びＯＳとアプリケーションとの関係を示す図である。

【図３】

アクセス管理テーブルのデータ構成例を示す図である。

【図４】

本発明におけるＡＰＩの監視／制御の第１の基本型を示すシーケンス図である。

【図５】

本発明におけるＡＰＩの監視／制御の第２の基本型を示すシーケンス図である。

【図６】

アクセス履歴を記録する機能を示すブロック構成図である。

【図７】

不正アクセスを示す画面例である。

【図８】

アクセス監視履歴の表示画面の例を示す図である。

図である。

【図９】

アクセス制限対象となるリソースの例を示す図である。

【図１０】

Ｈ．Ｈサイト、サーバの構成を示す第２実施形態の図である。

【図１１】

ＳＣＭとＯＳ、ファイル、外部装置との関係を示す図である。

【図１２】

全体のシステム構成を示す第３の実施形態の図である。

【図１３】

イントラネットへの応用を示す第４の実施形態である。

【図１４】

ホームでの応用を示す第５の実施形態である。

【図１５】

ユーザ、クライアントへの制限と課金のプロセスを示すフロー図である。

アクセス制限対象となるリソースの例を示す図である。

【符号の説明】

１０１　コンピュータ

１０２　ネットワーク

２０１　汎用ＯＳ

２０３　リソース管理プログラム

６０１　履歴管理プログラム

６０３　通報プログラム

２０３１　ＡＰＩ監視コントローラ

２０３２　ＡＰＬ監視コントローラ

２０３３　アクセス制御コントローラ

２０３４　ＯＳ監視コントローラ

２０３５　アクセス権管理テーブル

１１　Ｈ．Ｈサーバのアーキテクチャ

１２　管理テーブルファイル

１３　アプリケーションソフトウエアのファイル

１４　アクセス履歴記録、管理ファイル

１５　通信ネットワーク

１６　外部装置ドライバーソフト

１７　汎用ＯＳ

１８　ＡＰＩ１（Ａｐｐｌｉｃａｔｉｏｎ　Ｐｒｏｇｒａｍ　Ｉｎｔｅｒｆａｃｅ　１）

１９．ＳＣＭ（Ｓｅｃｕｒｉｔｙ　Ｃｏｎｔｒｏｌ　Ｍａｎｅｇｅｍｅｎｔ）

２０　ＡＰＩ２（Ａｐｐｌｉｃａｔｉｏｎ　Ｐｒｏｇｒａｍ　Ｉｎｔｅｒｆａｃｅ　２）

２１　ＡＰＬ（Ａｐｐｌｉｃａｔｉｏｎ　Ｐｒｏｇｒａｍ　Ｌｏｇｉｃ）

２２　外部機器インターフェース

２３　画面端末装置、ＴＶ、ＰＤＡ、大画面付多機能電話機

２４　プリンター

２５　Ｆａｘ／コピー機

２６　通信ライン

２７　コネクター、ケーブル

２８　ＰＣ、サーバ

３１　公式Ｗｅｂサイト

３２　無線基地局

３３　Ｈ．Ｈ（ハミングヘッズ）Ｗｅｂサイト

３４　データベースサイト

３５　Ｗｅｂキャスト、デジタル放送局

３６　銀行、金融機関、クレジット会社

３７　Ｗｅｂモール、インターネットショップ

３８　コンビニ、街角ターミナル

３９　学校、研究機関

４０　企業、工場、オフイス

４１　家庭、在宅就業

４２、７８　携帯情報端末機器、携帯電話機、ＰＤＡ

４３　ユーザ、クライアント

４４　車載移動端末機器

４５、７４　ホームサーバ

４６、７２　ホームルータ

５１　ルータ

５２　Ｗｅｂサーバ

５３　ファイヤウオール

５４　ＬＡＮ（Ｌｏｃａｌ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）

５５　Ｈ．Ｈサーバ

５６　情報格納ファイル

５７，５８，５８ｍｎ　ＰＣ、サーバ

５９、７５　多機能電話機

６０　Ｆａｘ、プリンター、コピー機

６１　携帯情報端末機器

６２　携帯電話機

６３　ノートＰＣ

６４　構内無線アンテナ

６５　構内移動車載端末機器

６６、６７　接続線

７１　ホーム無線アンテナ

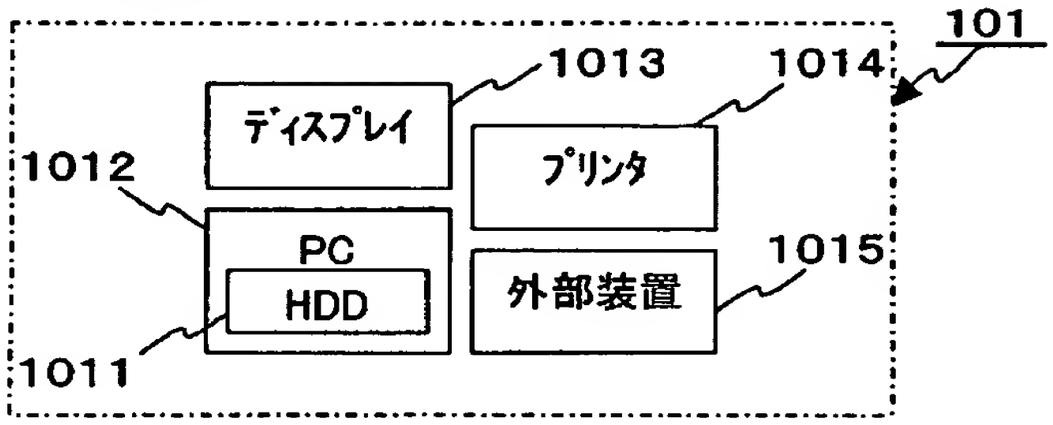
７７　音響機器

７６　ＴＶ

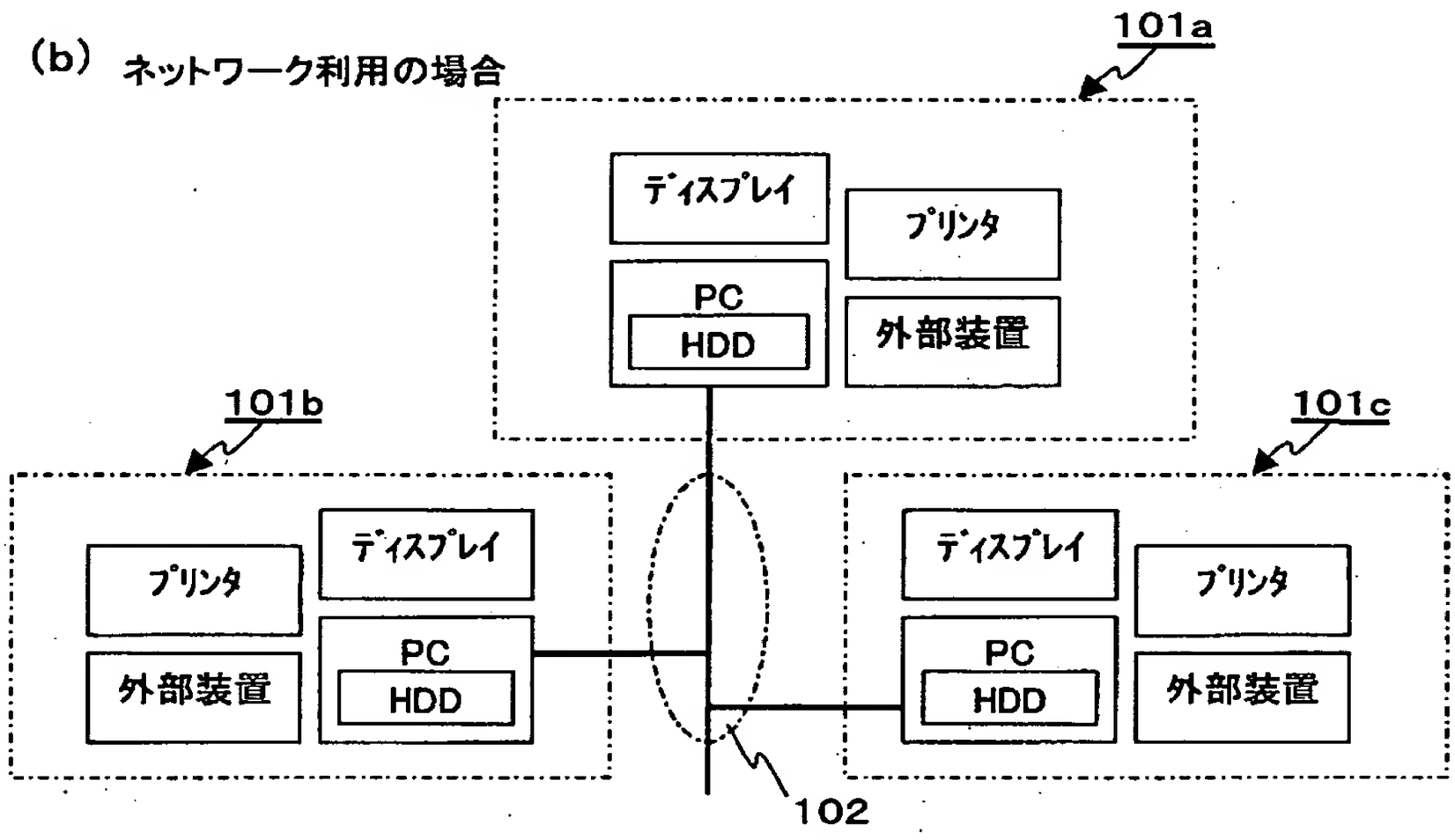
【書類名】　　図面

【図１】

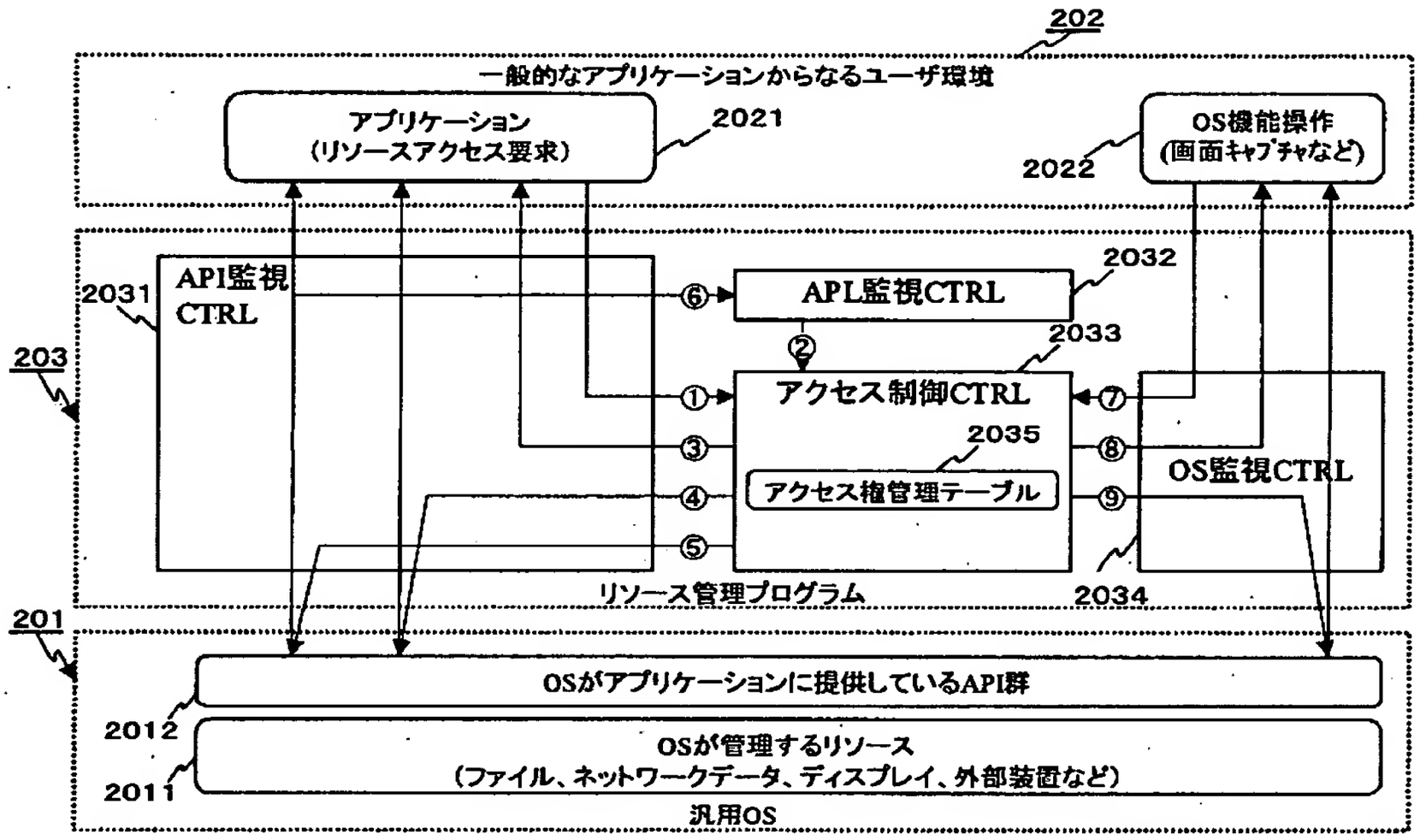
(a) スタンドアロンの場合



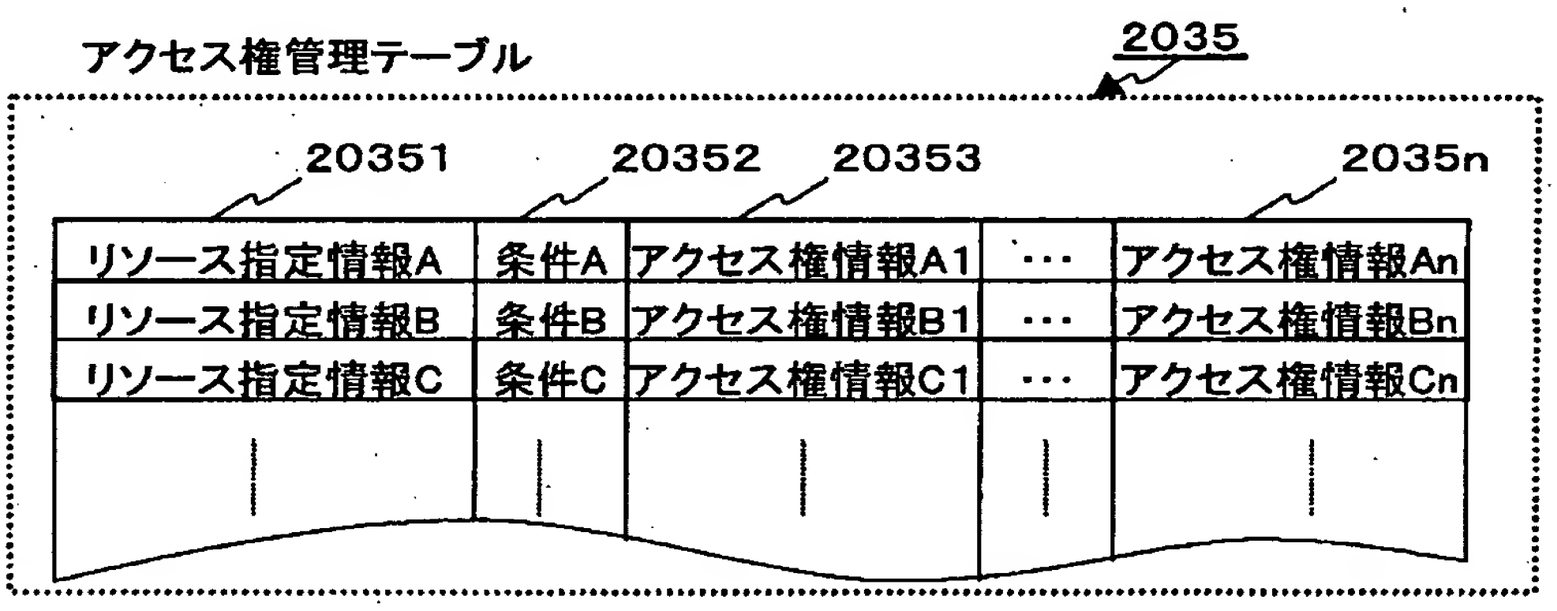
(b) ネットワーク利用の場合



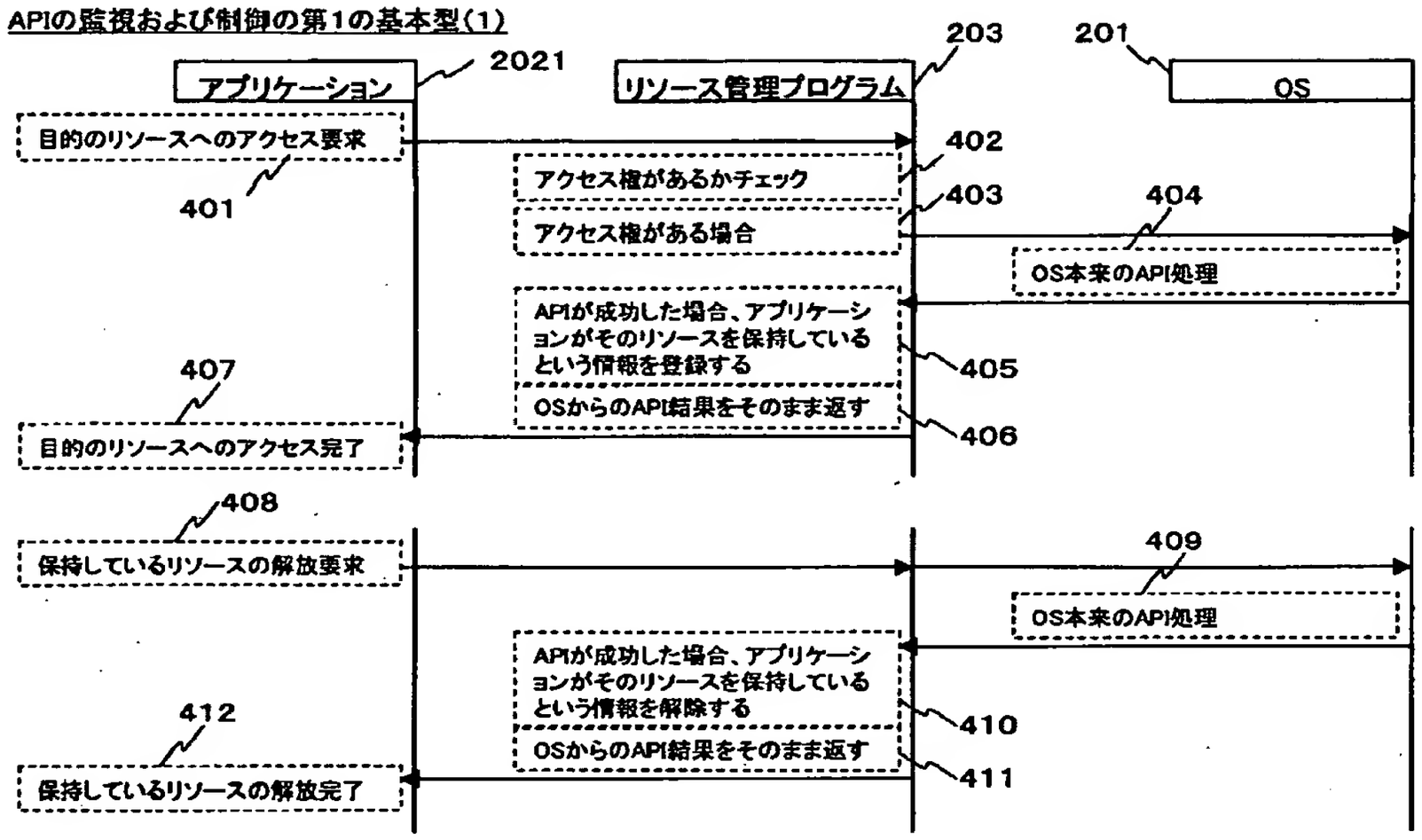
【図２】


202
一般的なアプリケーションからなるユーザ環境
アプリケーション
(リソースアクセス要求)
2021
OS機能操作
(画面ｷｬﾌﾟﾁｬなど)
2022
2031
API監視
CTRL
2032
APL監視CTRL
203
2033
アクセス制御CTRL
2035
アクセス権管理テーブル
OS監視CTRL
リソース管理プログラム
2034
201
OSがアプリケーションに提供しているAPI群
2012
OSが管理するリソース
(ファイル、ネットワークデータ、ディスプレイ、外部装置など)
2011
汎用OS

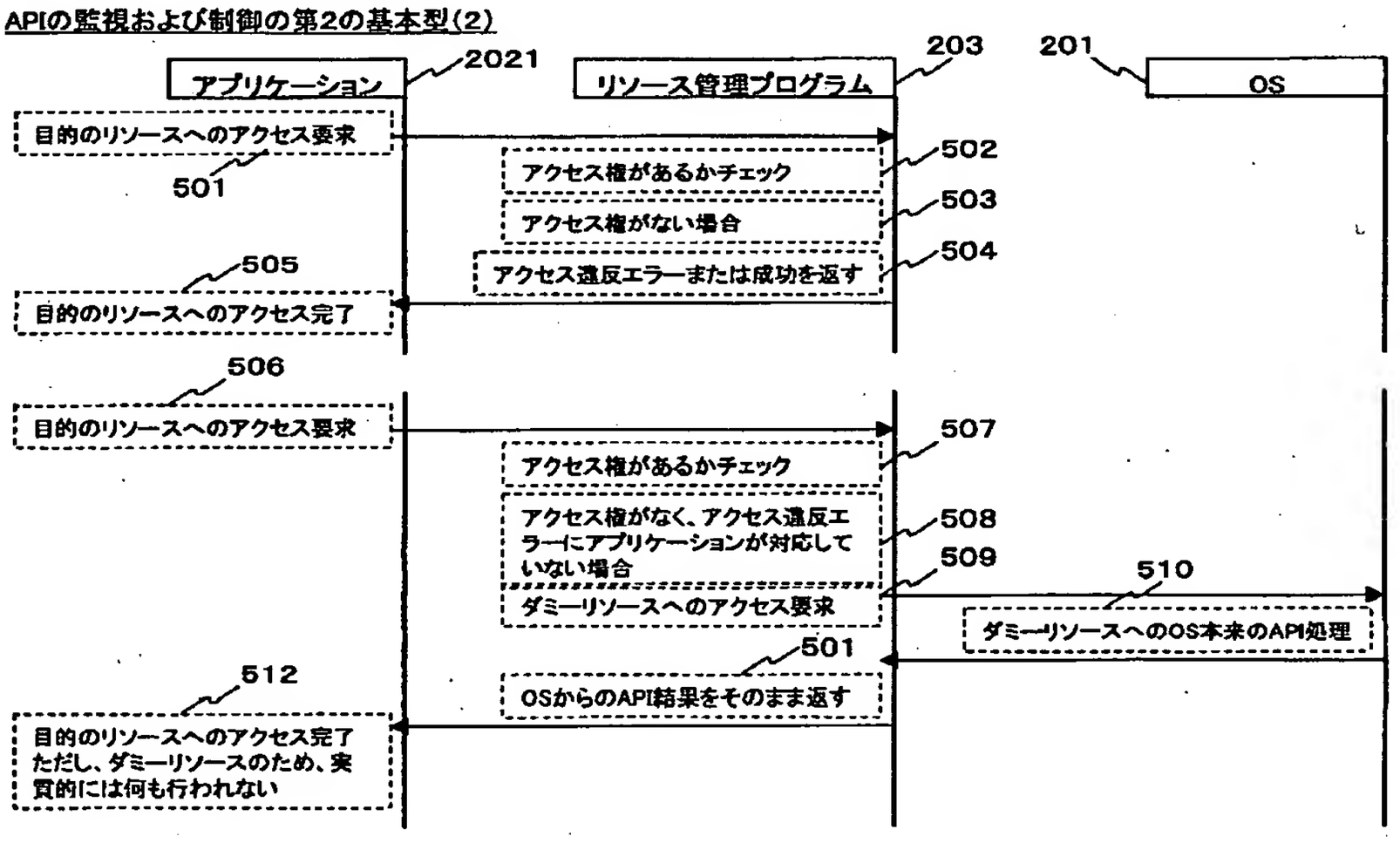
【図３】


アクセス権管理テーブル
2035
20351
20352
20353
2035n
リソース指定情報A
条件A
アクセス権情報A1
・・・
アクセス権情報An
リソース指定情報B
条件B
アクセス権情報B1
・・・
アクセス権情報Bn
リソース指定情報C
条件C
アクセス権情報C1
・・・
アクセス権情報Cn

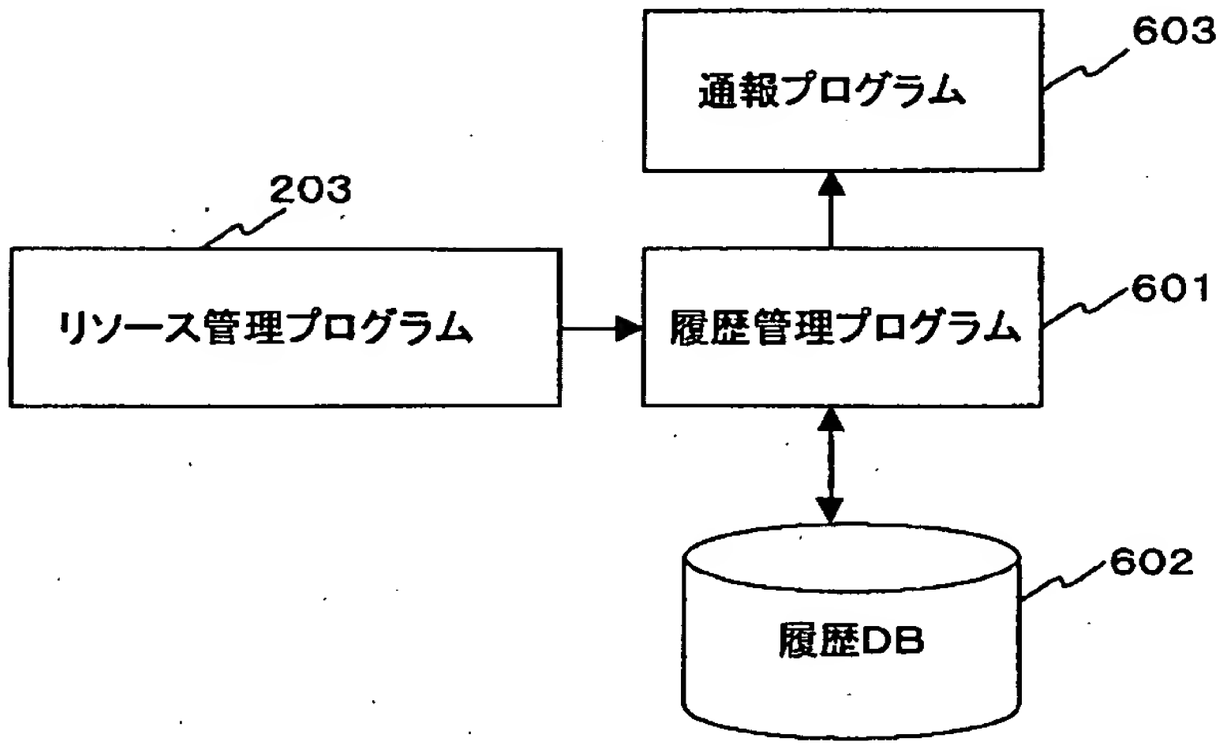
【図４】


APIの監視および制御の第1の基本型(1)
アプリケーション
2021
リソース管理プログラム
203
201
OS
目的のリソースへのアクセス要求
401
402
アクセス権があるかチェック
403
アクセス権がある場合
404
OS本来のAPI処理
APIが成功した場合、アプリケーションがそのリソースを保持しているという情報を登録する
405
407
OSからのAPI結果をそのまま返す
406
目的のリソースへのアクセス完了
408
保持しているリソースの解放要求
409
OS本来のAPI処理
APIが成功した場合、アプリケーションがそのリソースを保持しているという情報を解除する
410
412
OSからのAPI結果をそのまま返す
411
保持しているリソースの解放完了

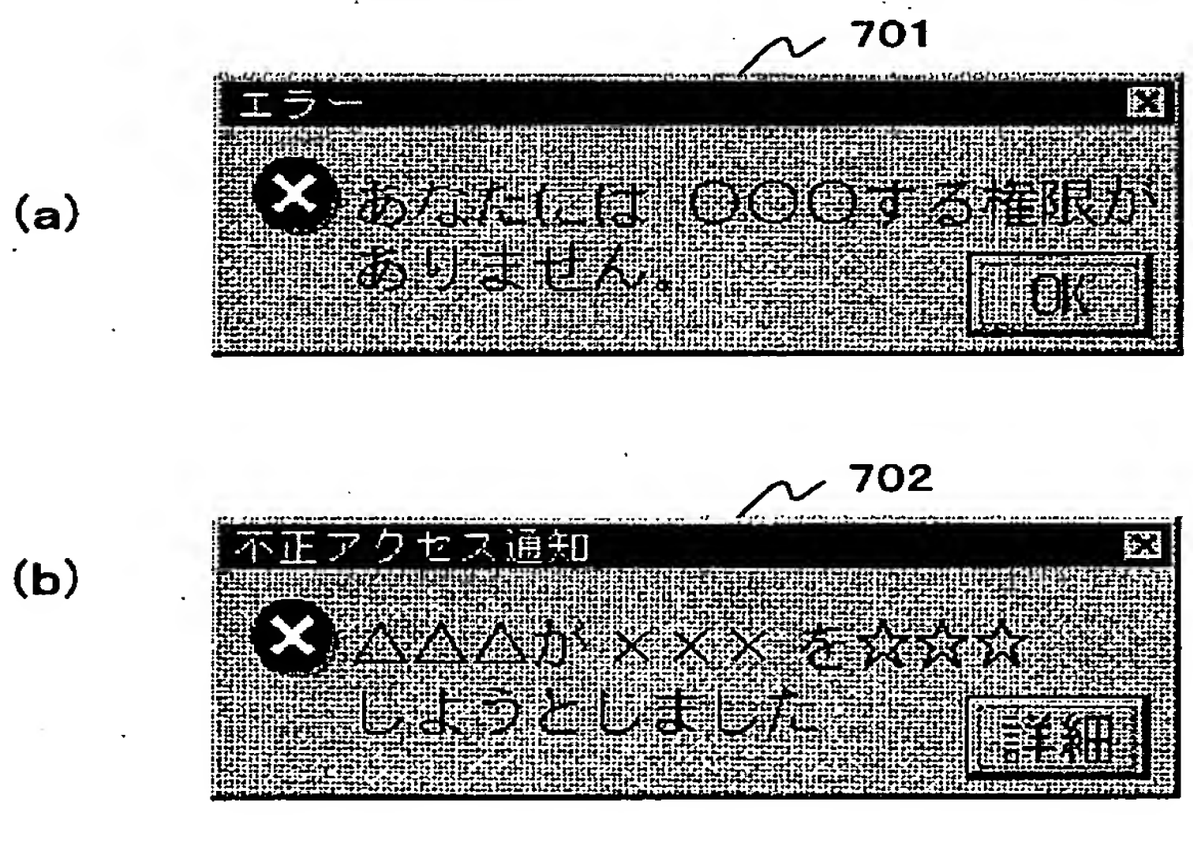
【図５】


APIの監視および制御の第2の基本型(2)
アプリケーション
2021
リソース管理プログラム
203
201
OS
目的のリソースへのアクセス要求
501
502
アクセス権があるかチェック
503
アクセス権がない場合
505
504
アクセス違反エラーまたは成功を返す
目的のリソースへのアクセス完了
506
目的のリソースへのアクセス要求
507
アクセス権があるかチェック
508
アクセス権がなく、アクセス違反エラーにアプリケーションが対応していない場合
509
510
ダミーリソースへのアクセス要求
ダミーリソースへのOS本来のAPI処理
501
512
OSからのAPI結果をそのまま返す
目的のリソースへのアクセス完了
ただし、ダミーリソースのため、実質的には何も行われない

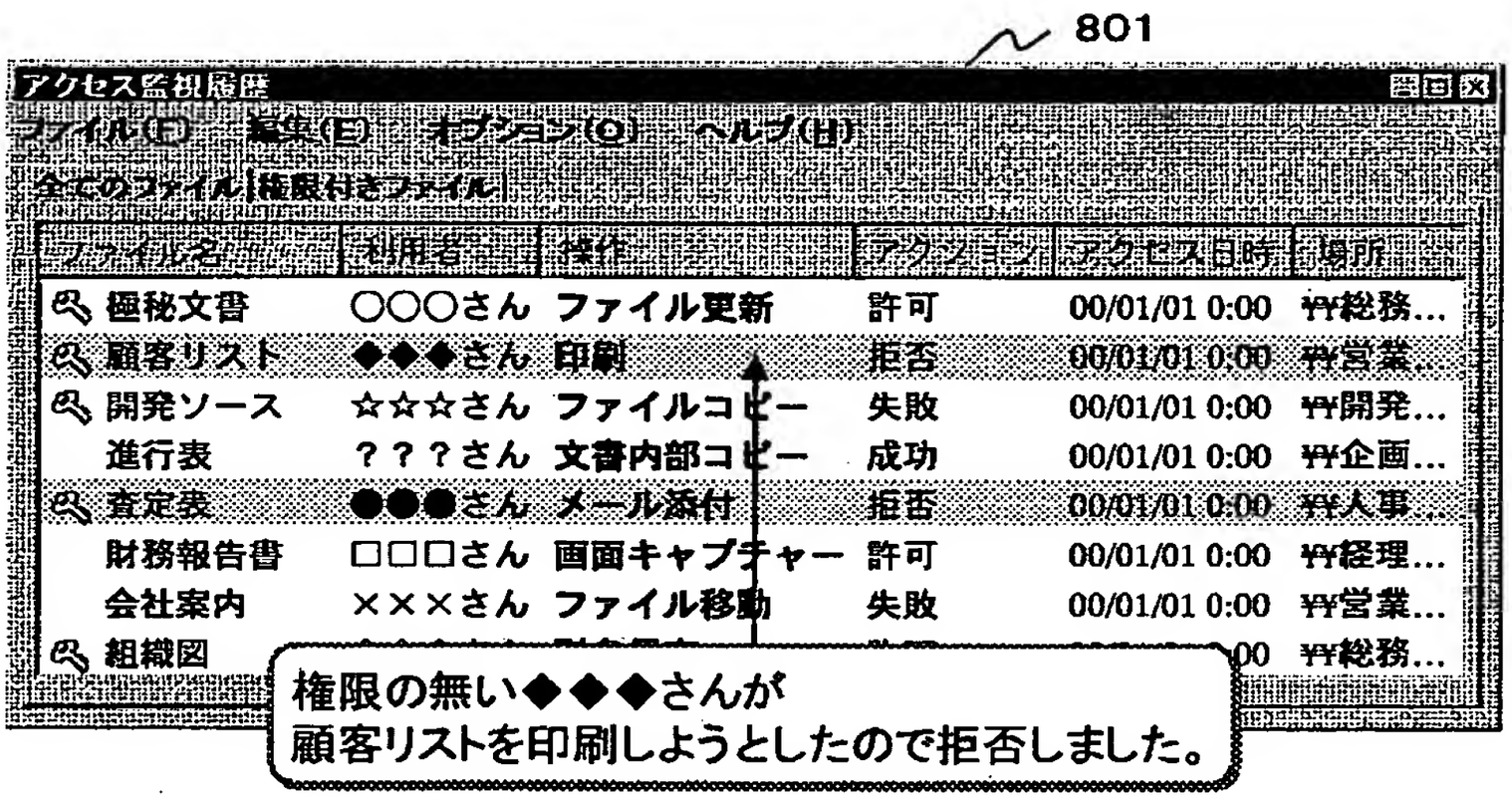
【図６】


通報プログラム
603
203
リソース管理プログラム
履歴管理プログラム
601
履歴DB
602

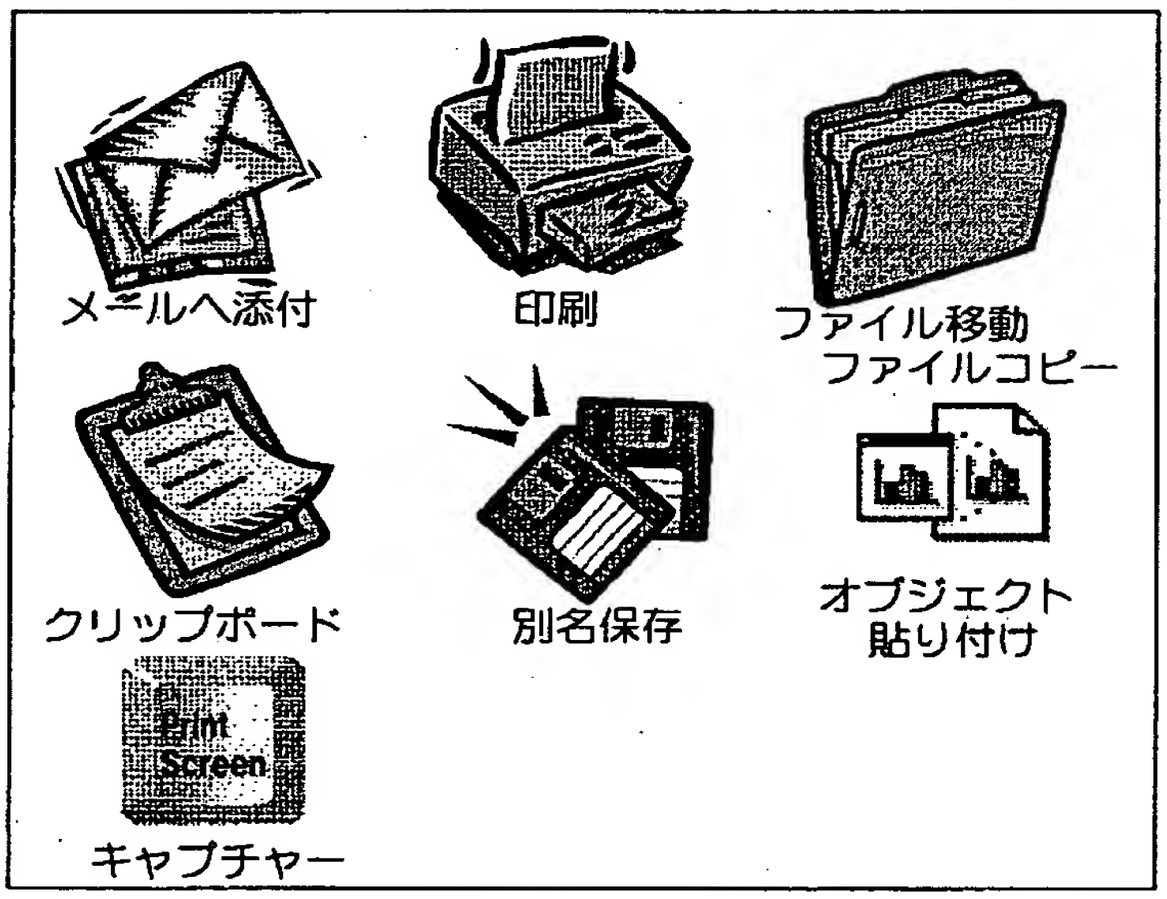
【図７】


(a)
701
エラー
あなたには ○○○する権限が
ありません。
OK
(b)
702
不正アクセス通知
△△△が ×××を ☆☆☆
しようとしました
詳細

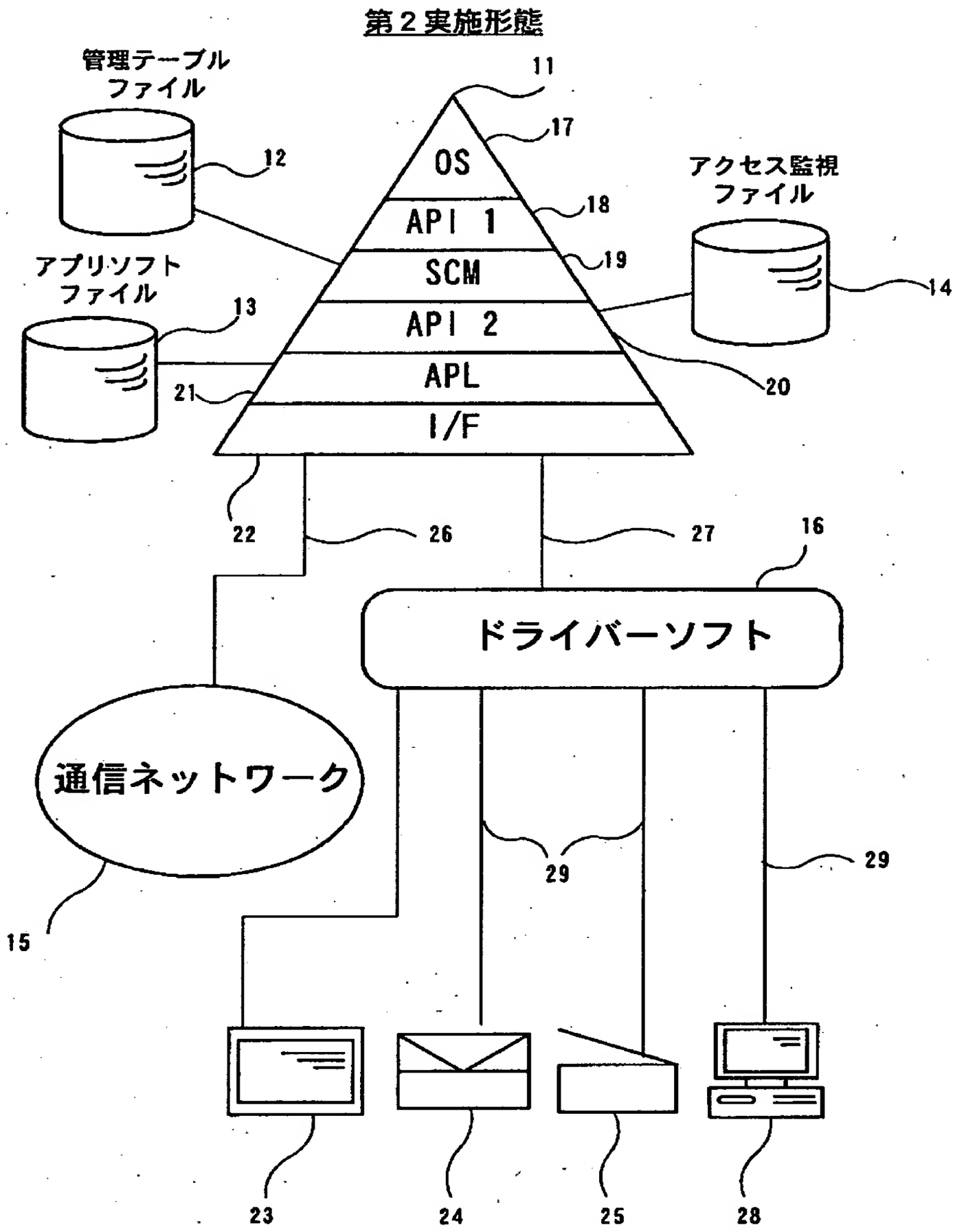
【図８】


801
アクセス監視履歴
ファイル(F)　編集(E)　オプション(O)　ヘルプ(H)
全てのファイル|権限付きファイル|
ファイル名　利用者　操作　アクション　アクセス日時　場所
極秘文書　○○○さん　ファイル更新　許可　00/01/01 0:00　¥¥総務...
顧客リスト　◆◆◆さん　印刷　拒否　00/01/01 0:00　¥¥営業...
開発ソース　☆☆☆さん　ファイルコピー　失敗　00/01/01 0:00　¥¥開発...
進行表　？？？さん　文書内部コピー　成功　00/01/01 0:00　¥¥企画...
査定表　●●●さん　メール添付　拒否　00/01/01 0:00　¥¥人事...
財務報告書　□□□さん　画面キャプチャー　許可　00/01/01 0:00　¥¥経理...
会社案内　×××さん　ファイル移動　失敗　00/01/01 0:00　¥¥営業...
組織図　00　¥¥総務...
権限の無い◆◆◆さんが
顧客リストを印刷しようとしたので拒否しました。

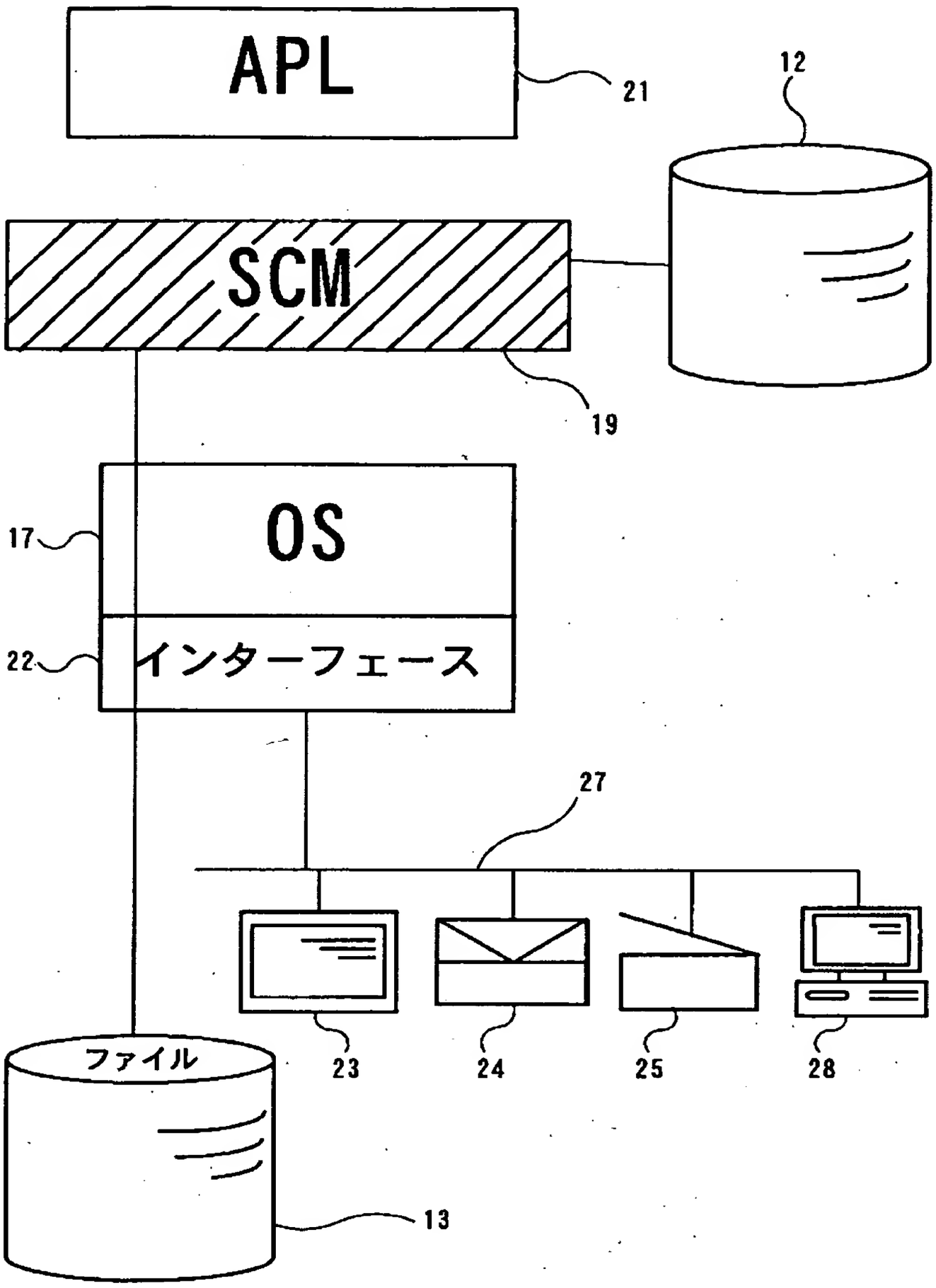
【図９】


メールへ添付
印刷
ファイル移動
ファイルコピー
クリップボード
別名保存
オブジェクト
貼り付け
Print Screen
キャプチャー

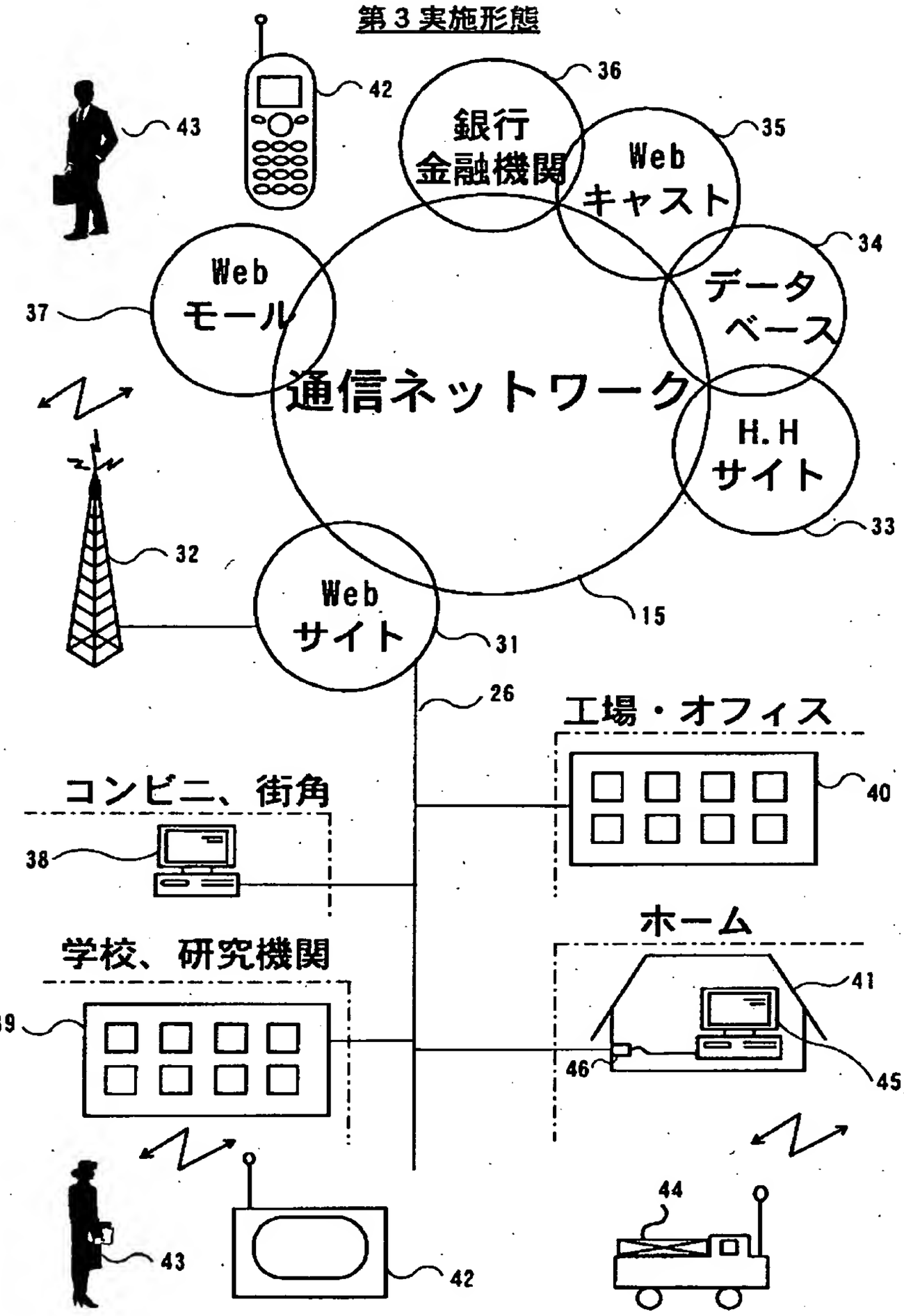
【図１０】


第２実施形態
管理テーブル
ファイル
12
アプリソフト
ファイル
13
11
17
OS
18
API 1
19
SCM
API 2
APL
I/F
21
20
アクセス監視
ファイル
14
22
26
27
16
ドライバーソフト
通信ネットワーク
15
29
29
23
24
25
28

【図１１】

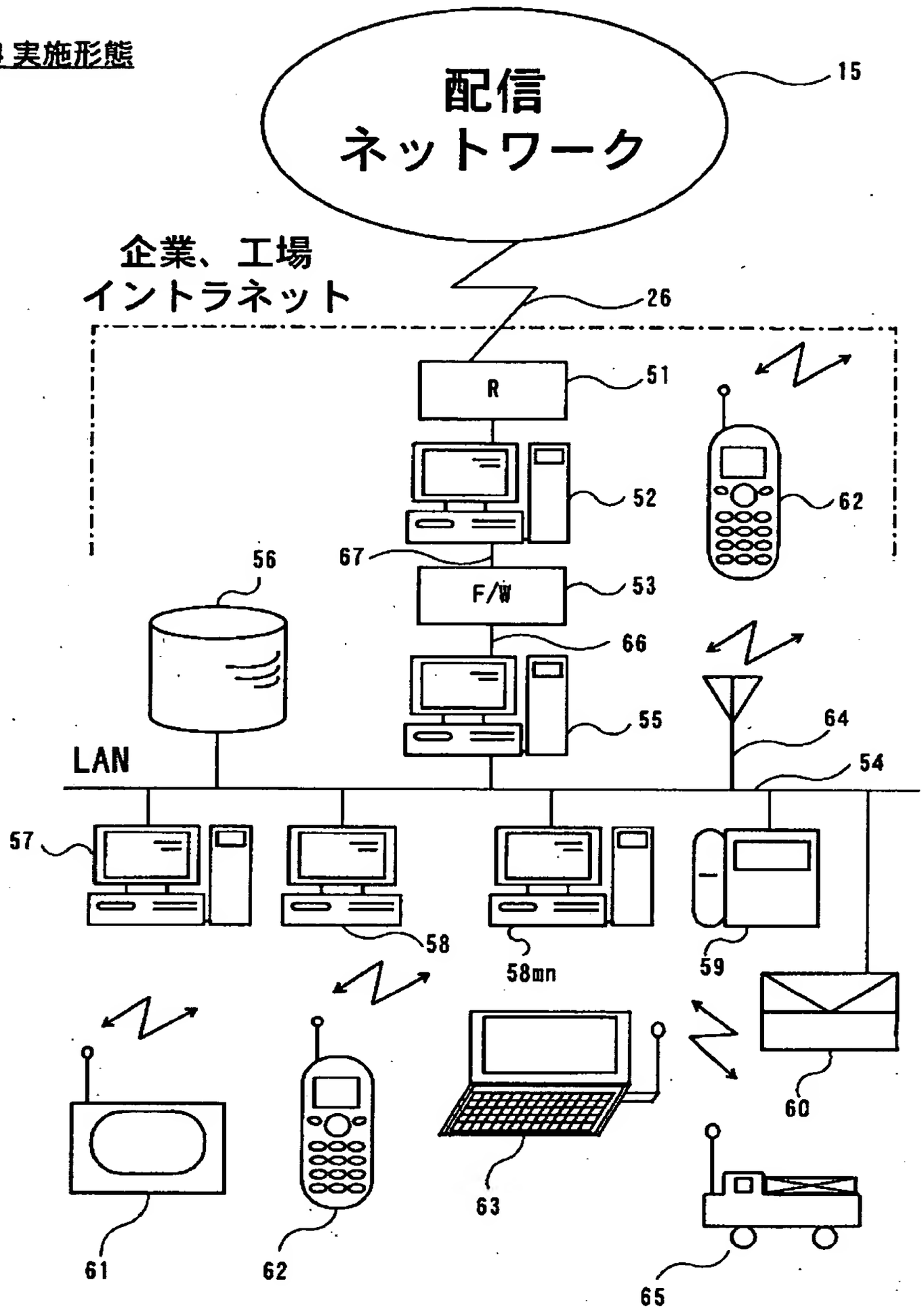


【図１２】

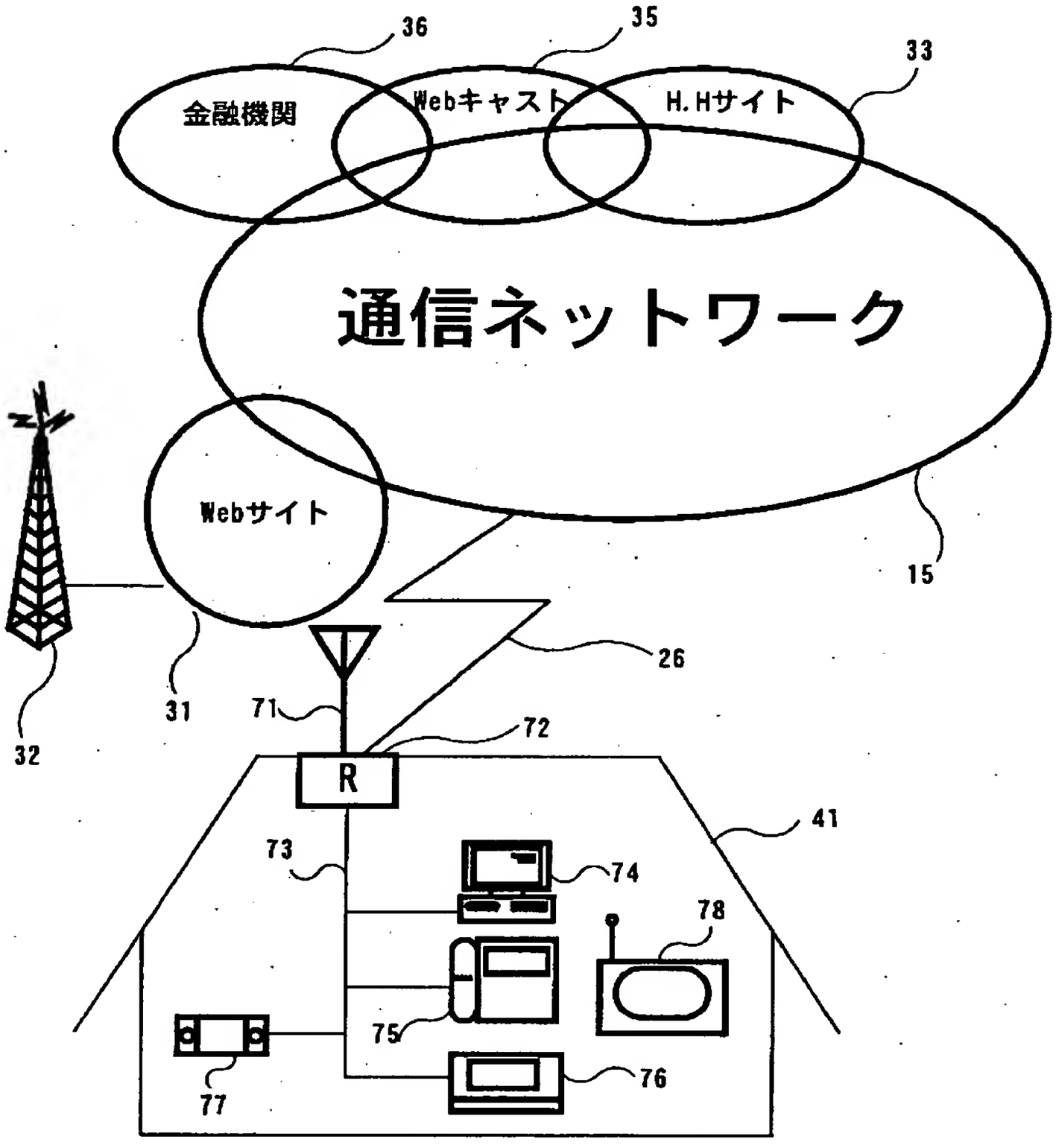

第３実施形態
銀行
金融機関
36
Web
キャスト
35
データ
ベース
34
H.H
サイト
33
Web
モール
37
通信ネットワーク
15
Web
サイト
31
32
26
工場・オフィス
40
コンビニ、街角
38
ホーム
41
45
学校、研究機関
39
46
44
43
42
43
42

【図１３】

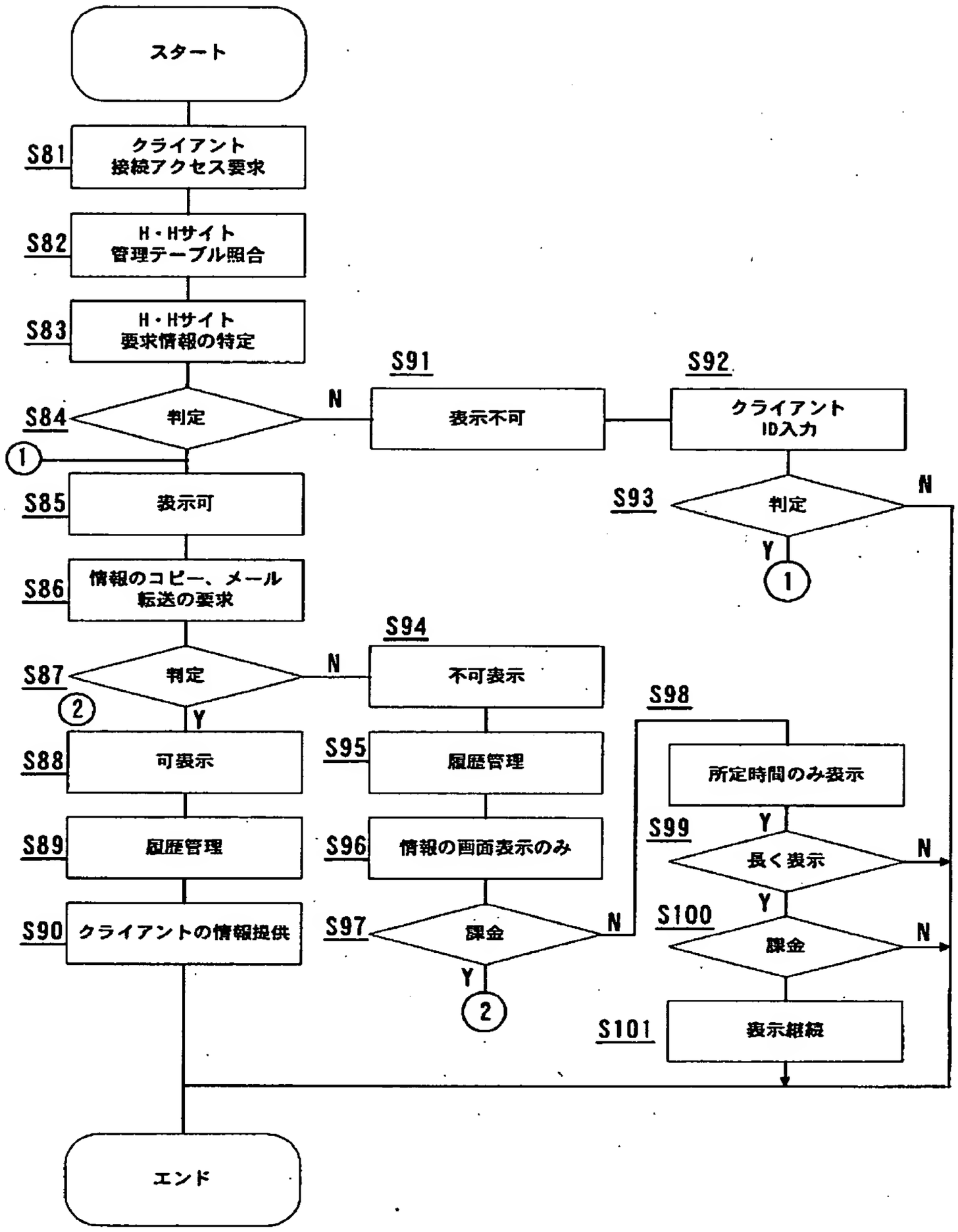
第４実施形態


配信
ネットワーク
15
企業、工場
イントラネット
26
R
51
52
62
67
56
F/W
53
66
55
64
LAN
54
57
58
58mn
59
61
62
63
60
65

【図１４】


第５実施形態(ホーム)
36
35
33
金融機関
Webキャスト
H.Hサイト
通信ネットワーク
Webサイト
15
26
31
71
72
32
R
41
73
74
78
75
77
76

【図１５】


スタート
S81
クライアント
接続アクセス要求
S82
H・Hサイト
管理テーブル照合
S83
H・Hサイト
要求情報の特定
S84
判定
N
S91
表示不可
S92
クライアント
ID入力
S93
判定
N
Y
①
①
S85
表示可
S86
情報のコピー、メール
転送の要求
S87
判定
N
S94
不可表示
②
Y
S88
可表示
S95
履歴管理
S89
履歴管理
S96
情報の画面表示のみ
S90
クライアントの情報提供
S97
課金
N
Y
②
S98
所定時間のみ表示
S99
長く表示
Y
N
S100
課金
Y
N
S101
表示継続
エンド

【書類名】　　要約書

【要約】

【課題】　ＯＳやプロセスを変更することなく、アクセス権限のないユーザに対するリソースの操作を制限し、しかも既存環境における禁止または制限事項を拡張すること。

【解決手段】　ファイル、ネットワーク、記憶装置、表示画面、外部付属装置等のオペレーティングシステムが管理しているコンピュータリソースに対するプロセスまたはオペレーティングシステムからの操作要求をコンピュータリソースにアクセスする前に捕捉し、その捕捉した操作要求によって指定されるコンピュータリソースに対するアクセス権限があるか否かを判定し、アクセス権限があれば当該操作要求通りにオペレーティングシステムに渡し、その結果を要求元プロセスに返し、アクセス権限がなければ当該操作要求を拒否するか、コンピュターリソースの内容に応じて課金する事によって許可する。

【選択図】　　図２

出　願　人　履　歴　情　報

識別番号　　〔５００００８３２２６〕

１．変更年月日　　２０００年　２月２５日
［変更理由］　新規登録
住　所　　東京都中央区月島１丁目２番１３号
氏　名　　ハミングヘッズ株式会社